Clavister Eagle E7
Getting Started Guide

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
www.clavister.com

Published 2015-04-07
Copyright © 2015 Clavister AB

Clavister Eagle E7
Getting Started Guide

Published 2015-04-07

Copyright © 2015 Clavister AB

Copyright Notice

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without the written consent of Clavister.

Disclaimer

The information in this document is subject to change without notice. Clavister makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Clavister reserves the right to revise this publication and to make changes from time to time in the content hereof without any obligation to notify any person or parties of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL CLAVISTER OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE CLAVISTER PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF CLAVISTER IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, CLAVISTER WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. CLAVISTER WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT CLAVISTER RECEIVED FROM THE END-USER FOR THE PRODUCT.

Table of Contents

Preface 5
1. E7 Product Overview 7
    1.1. Unpacking the E7 7
    1.2. Interfaces and Ports 9
2. Registering with Clavister 12
3. E7 Installation 17
    3.1. General Installation Guidelines 17
    3.2. Flat Surface Installation 19
    3.3. Rack Mounting 20
    3.4. Local Console Port Connection 23
    3.5. Micro-USB Console Port Connection 25
    3.6. Connecting Power 27
4. cOS Core Configuration 29
    4.1. Management Workstation Connection 29
    4.2. Web Interface and Wizard Setup 32
    4.3. Manual Web Interface Setup 40
    4.4. CLI Setup 56
    4.5. License Installation Methods 64
    4.6. Setup Troubleshooting 66
    4.7. Going Further with cOS Core 68
5. Resetting to Factory Defaults 71
6. Warranty Service 73
7. Safety Precautions 75
A. E7 Specifications 78
B. Declarations of Conformity 79
C. Port Based VLAN Setup 82

List of Figures

1.1. An Unpacked Clavister E7 Appliance 7
1.2. Clavister E7 Connection Ports 9
1.3. The E7 Ethernet Interface Ports 9
3.1. The E7 Micro-USB Local Console Port 25
3.2. E7 Power Inlet Socket 27

Preface

Target Audience

The target audience for this guide is the administrator who has taken delivery of a packaged Clavister E7 appliance and is setting it up for the first time. The guide takes the user from unpacking and installation of the device through to power-up, including network connections and initial cOS Core configuration.

There are two models of E7 appliance, a first generation and a second. The difference is that the first generation has an RJ45 console port and the second has a micro-USB port for console connection. This guide is for both models. However, all images show the second generation with micro-USB port.

Text Structure

The text is divided into chapters and subsections. Numbered subsections are shown in the table of contents at the beginning of the document.

Notes to the main text

Special sections of text which the reader should pay special attention to are indicated by icons on the left hand side of the page followed by a short paragraph in italicized text. There are the following types of such sections:

Note

This indicates some piece of information that is an addition to the preceding text. It may concern something that is being emphasized or something that is not obvious or explicitly stated in the preceding text.

Tip

This indicates a piece of non-critical information that is useful to know in certain situations but is not essential reading.

Caution

This indicates where the reader should be careful with their actions as an undesirable situation may result if care is not exercised.

Important

This is an essential point that the reader should read and understand.

Warning

This is essential reading for the user as they should be aware that a serious situation may result if certain actions are taken or not taken.

Text links

Where a "See section" link is provided in the main text, this can be clicked on to take the reader directly to that reference. For example, see *Section 4.6, "Setup Troubleshooting "*.

Web links

Web links included in the document are clickable. For example, *http://www.clavister.com*.

Trademarks

Certain names in this publication are the trademarks of their respective owners.

cOS Core is the trademark of Clavister AB.

Windows, *Windows XP*, *Windows Vista* and *Windows 7* are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Apple, *Mac* and *Mac OS* are trademarks of Apple Inc. registered in the United States and/or other countries.

Chapter 1: E7 Product Overview

• Unpacking the E7, page 7

• Interfaces and Ports, page 9

1.1. Unpacking the E7

Figure 1.1. An Unpacked Clavister E7 Appliance

This section details the unpacking of the E7 appliance. Open the packaging box used for shipping and carefully unpack the contents. The delivered product packaging should contain the following:

- The Clavister E7 appliance.
- RS-232 null modem cable **or** micro-USB console cable, depending on version. The E7 revision **A** has an RS-232 console connection. The E7 revision **B** has a micro-USB console connection.
- RJ45 Ethernet cable.
- Power cable and power supply.

Note: If any items are missing

If any items are missing from the E7 package, please contact the reseller or distributor. All relevant documentation in PDF format can be downloaded from the Clavister website and is included in the ZIP file distributions of new cOS Core versions.

Downloadable E7 Documentation

All documentation and other resources for the E7, including this guide, can be downloaded from the E7 product page which can be found at ***http://www.clavister.com/start***.

End of Life Treatment

The E7 appliance is marked with the European *Waste Electrical and Electronic Equipment* (WEEE) directive symbol which is shown below.

The product, and any of its parts, should not be discarded of by means of regular refuse disposal. At end-of-life, the product and parts should be given to an appropriate service that deals with the removal of such specialist materials.

1.2. Interfaces and Ports

This section is an overview of the E7 product's external design.

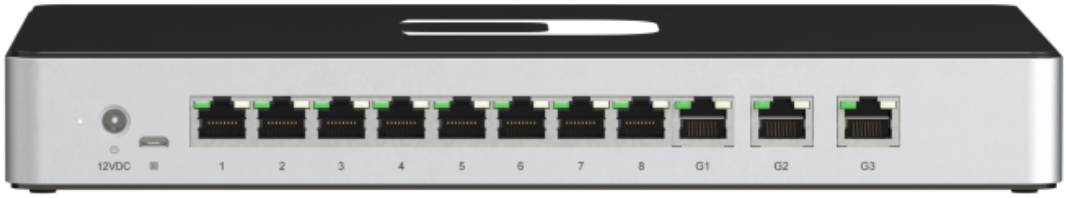


Figure 1.2. Clavister E7 Connection Ports

The E7 features the following connection ports on the front panel:

- On the left there is a set of RJ45 Gigabit Ethernet interfaces which are numbered **1** to **8**. All 8 interfaces are connected together by a common switch fabric and share the single logical cOS Core interface name **GESW**. This means that any security policy in the cOS Core rule sets that refers to the interface **GESW** will apply to traffic on any of the 8 physical interfaces.

  The **GESW** interfaces allow the configuration of *Port Based VLANs* through cOS Core so that the 8 interfaces can be divided up into different VLANs. This feature is described further in *Appendix C, Port Based VLAN Setup*.

- Next, are 3 x RJ45 Gigabit Ethernet interfaces. These have the logical cOS Core names of **G1**, **G2** and **G3**. The names are marked on each interface. These interfaces function independently of each other and are not connected by a switch fabric.

- There are two versions of the E7 appliance. The first generation version (revision **A**) provides console connection through an RS-232 RJ45 connector port. The second generation version (revision **B**) uses a micro-USB port. All images in this manual show only the micro-USB port version.

  The console port is used for direct access to the cOS Core *Boot Menu* and the cOS Core *Command Line Interface* (CLI). Access can be password protected.

All E7 Ethernet interfaces are capable of link speed auto-negotiation and can operate using 10Base-T, 100Base-Tx, or 1000Base-T.

Figure 1.3. The E7 Ethernet Interface Ports

All the E7 Ethernet interfaces support *Automatic MDI-X* and do not require a crossover cable for direct connection from another computer.

The full connection capabilities of all E7 Ethernet interfaces are listed in *Appendix A, E7 Specifications*.

Port Based VLAN

For the E7 only, cOS Core allows the administrator to configure of any of the **GESW** interfaces so

they act as a VLAN. All 8 Ethernet interfaces can act as 8 separate VLANs or they can be grouped into a lesser number of VLANs. Alternatively, some may be part of a VLAN and some may continue to act as normal **GESW** interfaces connected by a switch fabric. After such configuration, the VLAN processing load for these interfaces is handled by the E7 hardware without affecting cOS Core performance.

This feature is referred to as *Port Based VLAN* and is described in more detail in *Appendix C, Port Based VLAN Setup*.

Ethernet Interface Status LEDs

On the E7 there are indicator lights at the top left and top right of each interface which illuminate according to link status and activity. The conditions shown are:

- The top-left flashes green to indicate data traffic.
- The top-right light is green if the link is 10 or 100 Mb.
- The top-right light is amber if the link is 1 Gb.

Note: The GESW interface cannot be used with link aggregation

*If the cOS Core **link aggregation** feature is used, the logical **GESW** interface cannot be part of a **LinkAggregation** object.*

Chapter 2: Registering with Clavister

Before applying power to the E7 and starting cOS Core, it is important to understand the the customer and product registration procedures. There are two types of registration:

- **Registering as a Clavister Customer**

  This involves registering basic contact and company information on the Clavister website and establishing login credentials. Later, these credentials can also be used by cOS Core for automatically registering the E7 hardware unit and automatically downloading the correct license.

  This is is a mandatory requirement for all new customers and needs to be done only once. A description of doing this can be found below. Even if registration is not done before starting the cOS Core wizard, the wizard will provide a link to the registration page so it can be done while the wizard is running.

- **Registration of the E7 Hardware Unit**

  This is mandatory for every hardware unit before a license can be downloaded. It can be done in the following ways:

  i. **Automatic registration after cOS Core starts** - This can done by the *Setup Wizard* which starts automatically in a browser popup window when cOS Core Web Interface is started for the first time. The wizard is described in *Section 4.2, "Web Interface and Wizard Setup"*.

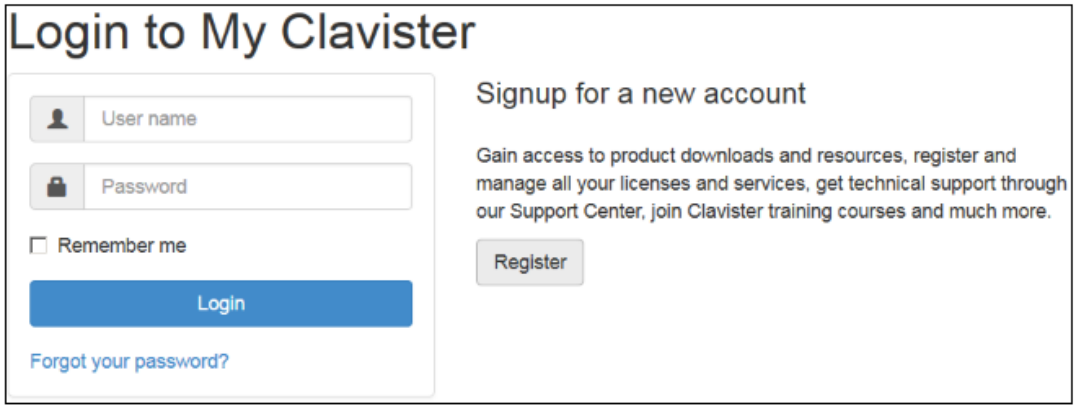
  ii. **Manual registration of the E7 on the Clavister website** - This is described in the last half of this section. Manual registration may be necessary if the E7 does not have Internet access.

A. Registering as a Clavister Customer

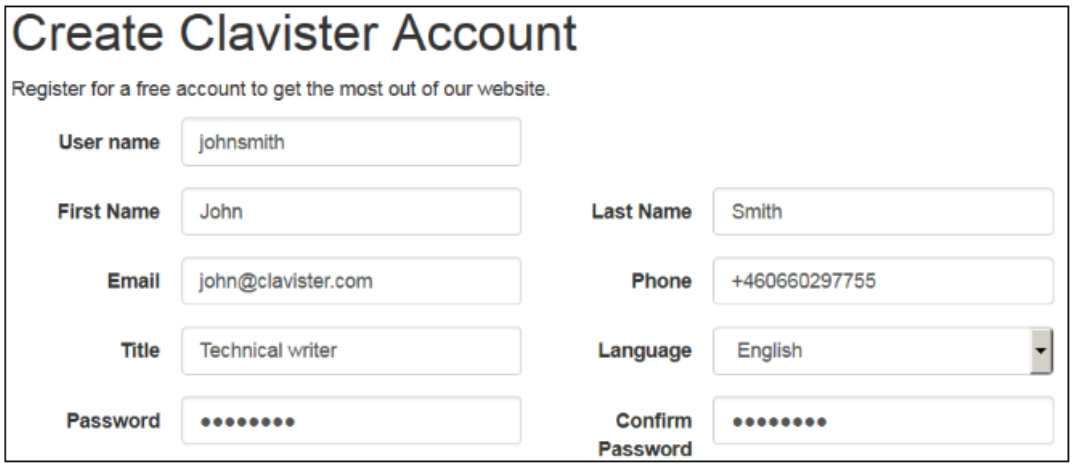
The E7 registration steps for a first time user of Clavister hardware are as follows:

1. Open a web browser, surf to ***http://www.clavister.com*** and select **Log in**.

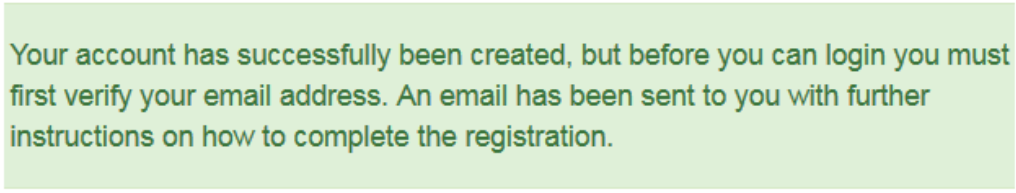
2. The customer login page is presented. It is assumed that a new customer is accessing the site for the first time so they should press the **Register** button. If already registered, log in and skip to step **8**.


Login to My Clavister
User name
Password
Remember me
Login
Forgot your password?
Signup for a new account
Gain access to product downloads and resources, register and manage all your licenses and services, get technical support through our Support Center, join Clavister training courses and much more.
Register

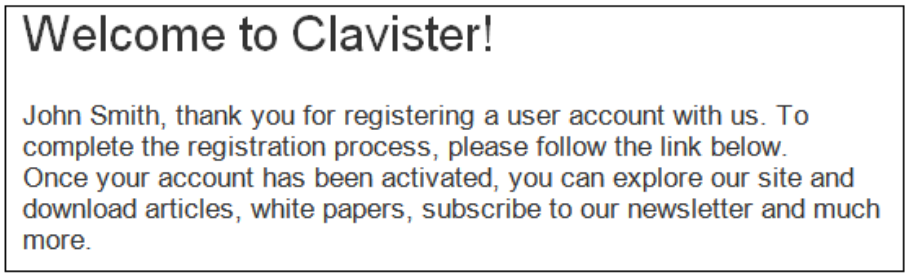
3. The registration webpage is now presented. The required information should be filled in. In the example below, a user called *John Smith* registers. It is important to enter the administrator's company details as well. Without company details, a license cannot be created.



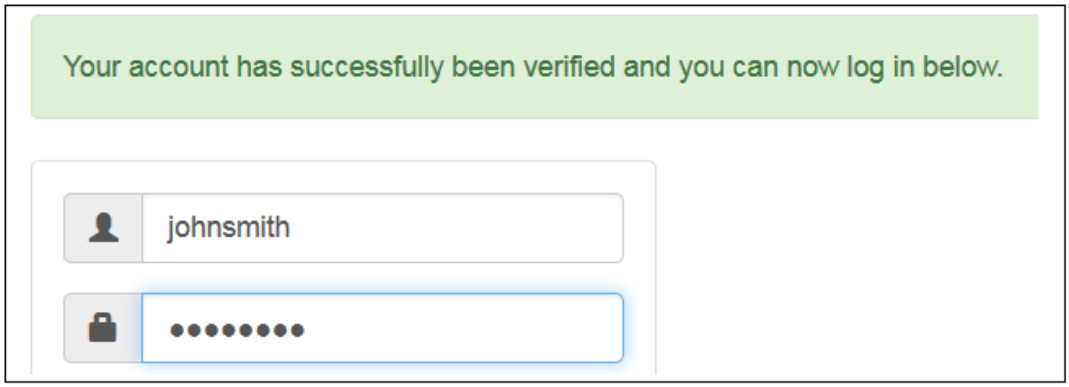
4. When the registration details are accepted, an email is sent to the email address given so that the registration can be confirmed.


Your account has successfully been created, but before you can login you must first verify your email address. An email has been sent to you with further instructions on how to complete the registration.

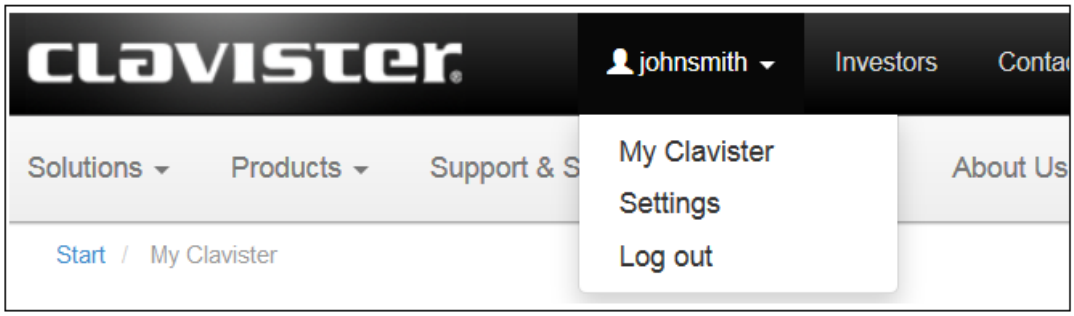
5. Below is an example of the email that John Smith would receive.


Welcome to Clavister!
John Smith, thank you for registering a user account with us. To complete the registration process, please follow the link below.
Once your account has been activated, you can explore our site and download articles, white papers, subscribe to our newsletter and much more.

6. When the confirmation link in the email is clicked, the new customer is taken to a webpage to indicate that confirmation has been successful. They should now log in to the Clavister website with the credentials they have submitted during registration.



7. After logging in, the website toolbar will show the name of the currently logged in customer.

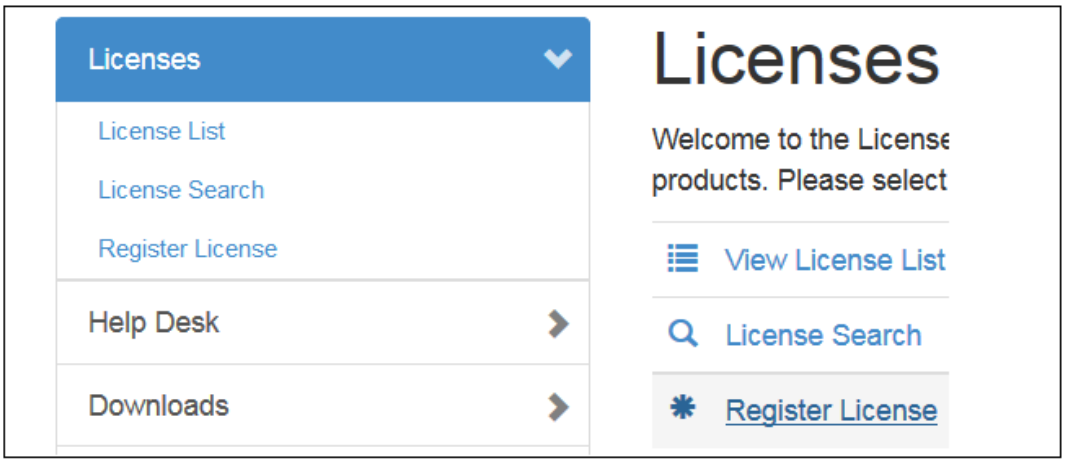


B. Registration of the E7 Hardware Unit

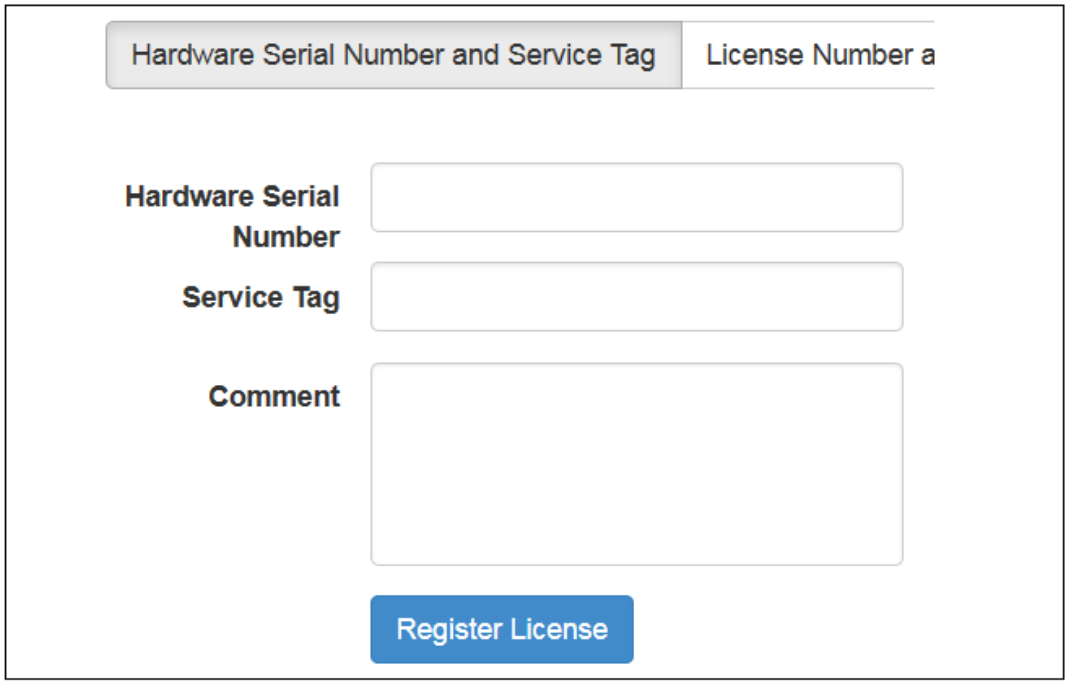
These steps describe manual registration of the E7 hardware unit.

Alternatively, if the E7 is connected to the Internet then this registration can be also be performed automatically by the cOS Core *Setup Wizard* which will appear as a browser popup window in the Web Interface when cOS Core starts for the first time.

1. Log in to the Clavister website and select the **Register License** option.



2. The registration page is displayed. Under the tab **Hardware Serial Number and Service Tag**, enter the *Hardware Serial Number* and *Service Tag* must be entered. **These two codes are found on a label which should be attached to the E7 hardware itself**. The label is usually found on the hardware's underside but may by found in another position.



clavister
Model: X00 Rev: A
Serial: X00A00101
Service-Tag: X1YZ-A1B2
Rated Input: 100-240 VAC/50-60 Hz/1A
Developed in Örnsköldsvik, Sweden. Manufactured in Xxxxxxx.
This device complies with Part 15 of the FCC Rules. Operation is subject too the following two conditions:
(1) This Device may not cause harmful interference and
(2) this device must accept any interference received including interference that may cause undesired operation.

The image above shows an example label which illustrates the typical layout of identification labels found on Clavister hardware products.

After Successful Hardware Registration

Once the E7 hardware unit is registered, a cOS Core license for the unit becomes available for download and installation from Clavister servers. This installation can be done automatically through the cOS Core *Setup Wizard* which is described in *Section 4.2, "Web Interface and Wizard Setup"*.

If the E7 is not connected to the Internet, the license must be manually downloaded from the cOS Core website and then manually uploaded.

All license installation options are listed and discussed in *Section 4.5, "License Installation Methods"*.

Chapter 3: E7 Installation

• General Installation Guidelines, page 17

• Flat Surface Installation, page 19

• Rack Mounting, page 20

• Local Console Port Connection, page 23

• Micro-USB Console Port Connection, page 25

• Connecting Power, page 27

3.1. General Installation Guidelines

Follow these geneneral guidelines when installing your Clavister E7 appliance:

- **Safety**

  Take notice of the safety guidelines laid out in *Chapter 7, Safety Precautions*. These are specified in multiple languages.

- **Power**

  Make sure that the power source circuits are properly grounded and then use the power cord supplied with the appliance to connect it to the power source.

- **Using Other Power Cords**

  If your installation requires a different power cord than the one supplied with the appliance, be sure to use a cord displaying the mark of the safety agency that defines the regulations for power cords in your country. Such marks are an assurance that the cord is safe.

- **Power Overload**

  Ensure that the appliance does not overload the power circuits, wiring and over-current protection.

  To determine the possibility of overloading the supply circuits, add together the ampere ratings of all devices installed on the same circuit as the appliance and compare the total with the rating limit for the circuit. The maximum ratings for the E7 are listed in *Appendix A, E7 Specifications*.

- **Surge Protection**

  A third party surge protection device should be considered and is strongly recommended as a means to prevent electrical surges reaching the appliance. This is mentioned again in *Section 3.6, "Connecting Power"*.

- **Temperature**

  Do not install the appliance in an environment where the ambient temperature during operation might fall outside the specified operating range. This range is documented in *Appendix A, E7 Specifications*.

  The intended operating temperature range is "room temperature". That is to say, the temperature most commonly found in a modern office and in which humans feel comfortable. This is usually considered to be between 20 and 25 degrees Celsius (68 to 77 degrees Fahrenheit). Special rooms for computer equipment may use a lower range and this is also acceptable.

- **Airflow**

  Make sure that airflow around the appliance is not restricted.

- **Dust**

  Do not expose the appliance to environments with elevated dust levels.

Note: The specifications appendix provides more details

Detailed information concerning power supply range, operating temperature range and other operating details can be found at the end of this publication in ***Appendix A, E7 Specifications****.*

3.2. Flat Surface Installation

The E7 can be mounted on any appropriate stable, flat, level surface that can safely support the weight of the appliance and its attached cables.

Rubber feet on the E7 unit are pre-attached to the underside of the appliance for operation on a flat surface. This protects both the surface and the appliance from external damage as well as allowing air to circulate underneath the hardware during operation.

Caution: Always leave space around the appliance

Always ensure there is adequate space around the appliance for ventilation and access to operating switches and cable connectors. No objects should be placed on top of the casing.

The E7 can also be rack mounted using an optional kit which is described next in *Section 3.3, "Rack Mounting"*.

3.3. Rack Mounting

An optional *Rack Mount Kit* is available for the E7 for mounting the appliance in a 19-inch rack. This kit must be ordered as a separate product and is not included as standard. Included with the kit is the following:

- 1 x side bracket for rack mounting including 2 fitted hex screws.
- 1 x side bracket for rack mounting with PSU mounting space including 2 fitted hex screws.
- 1 x plastic cable tie for securing the PSU to the rack mount.

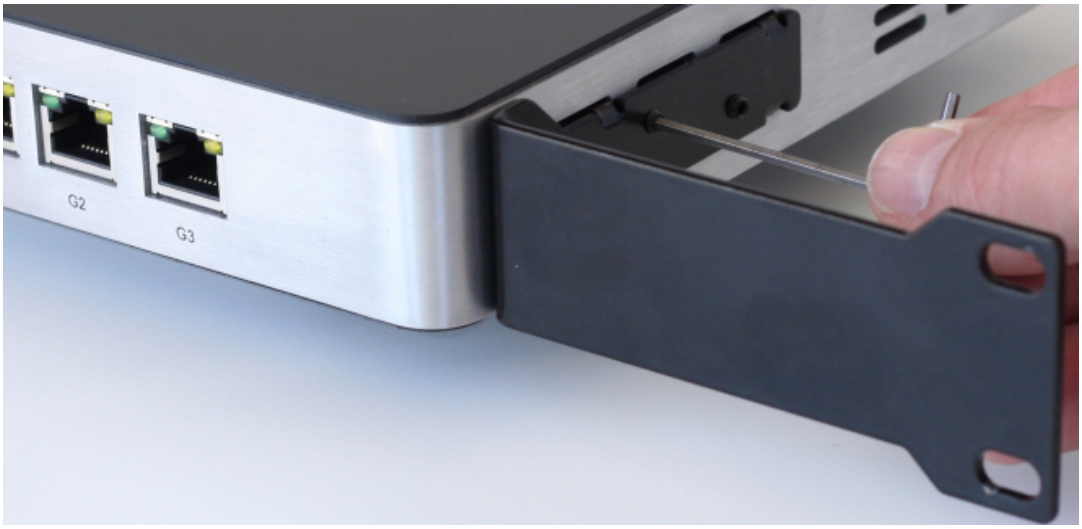
The kit is attached to the sides of the E7 unit prior to mounting in the rack. The steps for attaching the kit are as follows:

1. Take the bracket with the space for the power supply (PSU) and attached this to the E7 side nearest from the power inlet. Do this by slotting the brackets hooks into the fan vents on the side.

2. Push the bracket forward so it engages with the vents.

3. Take a Hex screw driver and secure the bracket by screwing in the 2 pre-installed screws. These screws will engage with the corners of the fan vents.

4. Take the second bracket without the PSU space and attached it to the other side of the E7 furthest from the power inlet in the same way. This is also secured by screwing the 2 pre-installed screws into the corners of the vents.



5. Take the external power supply and place it into the space provided on the PSU bracket. Gather the spare power cord into a bundle and secure this against the PSU as well as the PSU itself by looping the provided plastic cable tie around both, passing it through the holes provided in the bracket.

6. Finally, plug the PSU power cord into the E7 power inlet.

The E7 with the attached mounting brackets is now ready to be mounted in a 19-inch rack. Following mounting, the power cable can be plugged into the E7 PSU.

3.4. Local Console Port Connection

On the first generation of the E7 appliance (revision **A**) the *local console port* is a physical RJ45 RS-232 port on the front panel of the hardware. The second generation of E7 (revision **B**) provides a micro-USB port instead and connection with this is described in *Section 3.5, "Micro-USB Console Port Connection"*.

This local console port allows direct management connection to the appliance, either from a separate computer running console emulation software or from a console terminal. Local console access can then be used for both management of cOS Core with CLI commands or to enter the *boot menu* in order to access E7 firmware loader options.

Tip: Skip the rest of this section if using the Web Interface

This rest of this section can be initially skipped if cOS Core setup is going to be done with the cOS Core Web Interface since neither boot menu or CLI access will be needed.

Issuing CLI Commands

CLI commands can be issued via the local console port for both initial cOS Core setup as well as for ongoing system administration.

The local console port need not be used if setup is done through a web browser as described in *Section 4.2, "Web Interface and Wizard Setup"*. If the local console port is used for setup, no password is initially needed and the CLI commands required are described in *Section 4.4, "CLI Setup"*.

Note: Setting a local console password is recommended

A local console password need not be set. However, if it is not, anyone with physical access to the local console will have full administrator rights.

Unless the hardware is placed in a secure area, it is therefore recommended to set a local console password. This is done by entering the console ***boot menu*** *at system startup by pressing any console key before cOS Core has fully started. The boot menu and its options is discussed further in the separate* ***cOS Core Administrators Guide****.*

Requirements for Local Console Connection

To get management access via the local console port, the following is needed:

- A terminal or a computer with a serial port and the ability to emulate a terminal (for example, the open source *puTTY* software).
- The terminal console should have the following settings:
  i. 9600 bps.
  ii. No parity.
  iii. 8 bits.
  iv. 1 stop bit.

v. No flow control.

- An RS-232 cable with appropriate terminating connectors.

Connection Steps

To connect a terminal to the local console port, perform the following steps:

1. Check that the console connection settings are configured as described above.
2. Connect one of the connectors on the cable directly to the local console port on the E7.
3. Connect the other end of the cable to a console terminal or to the serial connector of a computer running console emulation software.

Connection Using SSH

An alternative to using the local console port for CLI access is to connect via a physical Ethernet interface and using a Secure Shell (SSH) client on the management workstation to issue CLI commands. This is discussed further in *Section 4.1, "Management Workstation Connection"*.

3.5. Micro-USB Console Port Connection

On the second generation of the E7 appliance (revision **B**) the *local console port* is a physical micro-USB port on the front panel of the hardware.

Figure 3.1. The E7 Micro-USB Local Console Port

This port allows direct management connection to the appliance from a separate computer running console emulation software. Console access can then be used for both management of cOS Core with CLI commands or to enter the *boot menu* in order to access E7 firmware loader options.

Tip: Skip the rest of this section if using the Web Interface

This rest of this section can be initially skipped if cOS Core setup is going to be done with the cOS Core Web Interface since neither boot menu or CLI access will be needed.

Connection Steps

To connect a computer to the local console port, perform the following steps:

1. Connect a micro-USB connector directly to the local console port on the E7.
2. Connect the other end of the cable to a USB port on computer running console emulation software.
3. After connection to a PC, Windows will try to recognize the device and automatically install the appropriate driver through the WIndows Update™ feature. If Windows is unable to do this automatically, it will present a link to a third-party web page where the driver can be downloaded.

   For the Linux and MacOS micro-USB drivers or to download the Windows driver separately, go to the E7 product page which can be found at ***http://www.clavister.com/start***.
4. Direct the console emulator on the computer to connect to the newly installed device. After successful connection, commands can be issued to the cOS Core *Command Line Interface* (CLI).

Issuing CLI Commands

CLI commands can be issued via the local console port for both initial cOS Core setup as well as for ongoing system administration.

The local console port need not be used if setup is done through a web browser as described in *Section 4.2, "Web Interface and Wizard Setup"*. If the local console port is used for setup, no password is initially needed and the CLI commands required are described in *Section 4.4, "CLI Setup"*.

Connection Using SSH

An alternative to using the local console port for CLI access is to connect via a physical Ethernet interface and using a Secure Shell (SSH) client on the management workstation to issue CLI commands. This is discussed further in *Section 4.1, "Management Workstation Connection"*.

Note: Setting a local console password is recommended

A local console password need not be set. However, if it is not, anyone with physical access to the local console will have full administrator rights.

Unless the hardware is placed in a secure area, it is therefore recommended to set a local console password. This is done by entering the console ***boot menu*** *at system startup by pressing any console key before cOS Core has fully started. The boot menu and its options is discussed further in the separate* ***cOS Core Administrators Guide****.*

3.6. Connecting Power

This section describes connecting power. As soon as power is applied, the E7 will boot-up and cOS Core will start.

Important

Please review the electrical safety information in ***Chapter 7, Safety Precautions****.*

Connecting AC Power

To connect power, follow these steps:

1. Plug the end of the power adapter's power cord into the power inlet socket on the E7.

Figure 3.2. E7 Power Inlet Socket

2. Plug the power adapter into a suitable AC power outlet. There is no On/Off switch and the unit will begin to boot up as soon as power is applied.

3. The E7 will boot up and cOS Core will start. After a brief period of time, cOS Core will be initialized and the E7 appliance is ready for configuration from a management workstation using either the *Web Interface* or the *Command Line Interface* (CLI) as the management interface.

   Initial configuration is discussed in detail in *Chapter 4, cOS Core Configuration*.

Important: Protecting Against Power Surges

It is recommended that the purchase and use of a separate surge protection unit from a third party is considered for the power connection to the E7 hardware. This is to ensure that the E7 is protected from damage by sudden external electrical power surges through the power cable.

Surge protection is particularly important in locations where there is a heightened risk of lightning strikes and/or power grid spikes.

Any surge protection unit should be installed exactly according to the manufacturer's instructions since correct installation of such units is vital for them to be effective.

Chapter 4: cOS Core Configuration

• Management Workstation Connection, page 29

• Web Interface and Wizard Setup, page 32

• Manual Web Interface Setup, page 40

• CLI Setup, page 56

• License Installation Methods, page 64

• Setup Troubleshooting , page 66

• Going Further with cOS Core, page 68

4.1. Management Workstation Connection

cOS Core Starts After Power Up

It is assumed that the E7 unit is now unpacked, positioned correctly and powered is applied. If not, the earlier chapters in this manual should be referred to before continuing.

Clavister's cOS Core network security operating system is preloaded on the E7 and will automatically boot up after power is applied. After boot-up is complete, an external management computer workstation can be used to configure cOS Core.

The Default Management Interface

After first time startup, cOS Core automatically makes management access available on a single predefined Ethernet interface and assigns the private IPv4 address **192.168.1.1** to it.

For the E7, the default management interface is any of the **GESW** interfaces since they are connected together by a switch fabric. By convention, the first interface (labeled **1**) is normally used for management workstation connection.

cOS Core Setup Methods

Initial cOS Core software configuration can be done in one of the following ways:

- **Through a web browser.**

  A standard web browser running on a standalone computer (also referred to as the *management workstation*) can be used to access the cOS Core *Web Interface*. This provides an intuitive graphical interface for cOS Core management. When this interface is accessed for the first time, a *setup wizard* runs automatically to guide a new user through key setup steps. The wizard can be closed if the administrator wishes to go directly to the Web Interface to perform setup manually.

  The wizard is recommended for its simplification of initial setup and is described in detail in *Section 4.2, "Web Interface and Wizard Setup"*. The wizard assumes that connection to the public Internet is one of the tasks to be performed and has a step for this.

- **Through a terminal console using CLI commands.**

  Alternatively, the setup process can be performed using console CLI commands and this is described in *Section 4.4, "CLI Setup"*. The CLI allows step by step control of setup and should be used by administrators who fully understand both the CLI and setup process.

  CLI access is possible in one of two ways:

  i. CLI access can be remote, across a network to a physical Ethernet interface. This is a similar to the connection used with the Web Interface and is also done using the default management interface after powering up for the first time.

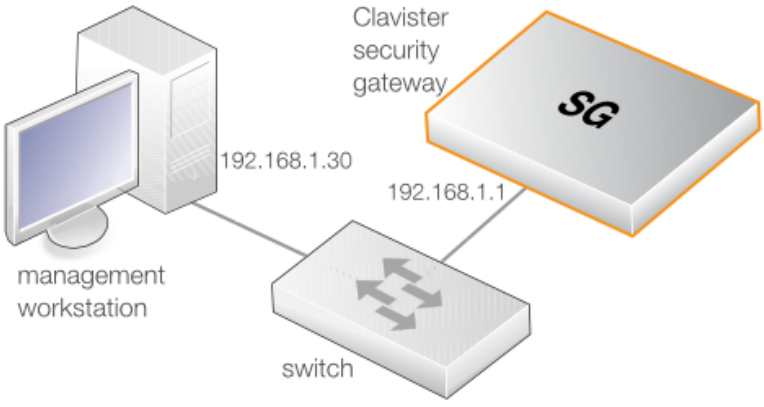
  ii. Alternatively, CLI access can be through console emulation software running on a Windows based computer connected directly to the micro-USB port on the E7 hardware. Direct console connection is described in *Section 3.5, "Micro-USB Console Port Connection"*. For first generation E7 models with an RJ45 local console port, direct console connection is described in *Section 3.4, "Local Console Port Connection"*.

Network Connection Setup

For setup using the Web Interface via a web browser or the CLI via SSH, it is necessary to connect an Ethernet interface on an external workstation computer to the default management Ethernet interface on the E7.

The default management Ethernet interface for the E7 is any of the **GESW** interfaces (as a convention, the first is normally used) and this is assigned the default IPv4 address of **192.168.1.1** by cOS Core. This interface should be connected to the same network as the management workstation (or a network accessible from the workstation via one or more switches).

Typically, the connection between the management workstation and the default management interface is made via a switch using standard Ethernet cables, as shown in the illustration below.



For connection to the public Internet, another E7 Ethernet interface should be connected to an ISP and this is referred to in the setup wizard as the *WAN* interface. In this guide, it is assumed that the physical **G2** interface of the E7 is used for Internet connection, although any other unused interface could be used instead.

Direct Connection to the Management Interface

Connection to the management interface from the workstation can be done directly without a switch. This could be done using a crossover cable. However, all the RJ45 interfaces on the E7 support *Automatic MDI-X* and a crossover cable is not necessary.

Workstation Ethernet Interface Setup

The only requirement for the Ethernet interface used for connection on the management workstation is that DHCP is enabled. cOS Core automatically enables a DHCP server on the security gateway's **GESW** interfaces and this allocates the required IP addresses to the workstation computer using DHCP.

If the workstation is configured manually, the following settings should be used:

- **IP address:** *192.168.1.30*
- **Subnet mask:** *255.255.255.0*
- **Default gateway:** *192.168.1.1*

Tip: Using another workstation interface IP address

*The IPv4 address assigned to the management workstation's Ethernet interface, could be any address from the **192.168.1.0/24** network. However, the IP chosen must be different from **192.168.1.1** which is used by cOS Core's default management interface.*

4.2. Web Interface and Wizard Setup

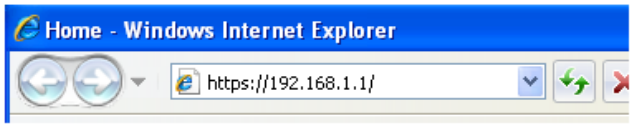
This chapter describes the setup when accessing cOS Core for the first time through a web browser. The user interface accessed in this way is called the *Web Interface*. It assumes that a physical network connection has been set up from a management computer to the default management Ethernet interface as described in *Section 4.1, "Management Workstation Connection"*.

Note: Some screenshot images have been clipped

Many of the images in this section are cut from original screenshots to condense the information presented. However, all relevant details in the images have been preserved.

Connect By Browsing to *https://192.168.1.1*

Using a web browser, enter the address *https://192.168.1.1* into the navigation window as shown below.



Important: Disable any proxy server and turn off popup blocking

Make sure the web browser doesn't have a proxy server configured.

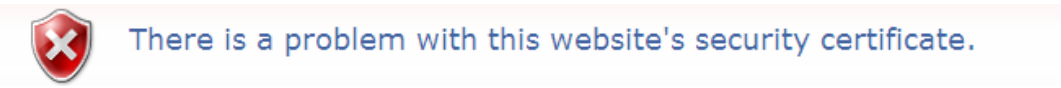
The wizard runs in a browser popup window. The popup must be allowed for the setup wizard to run.

If there is no response from cOS Core and the reason is not clear, refer to the help checklist in *Section 4.6, "Setup Troubleshooting "*.

The cOS Core Self-signed Certificate

When responding to an *https://* request, by default cOS Core sends a self-signed certificate which will not be initially recognized so it will be necessary to tell the browser to accept the certificate for this and future sessions.

Different browsers handle this self-signed certificate in slightly different ways. In Microsoft Internet Explorer the following error message will be displayed in the browser window.



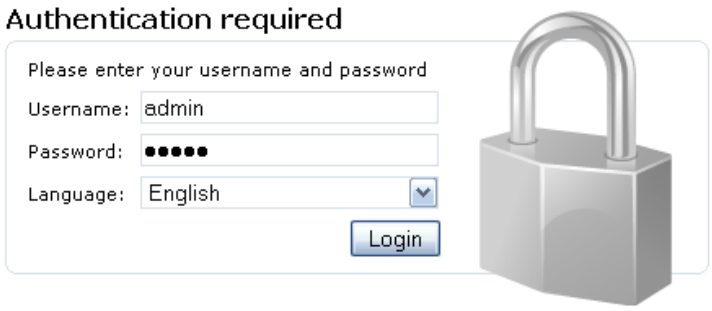
To continue, tell IE to accept the certificate by clicking the following link which appears near the bottom of the browser window.

In Firefox, this procedure is called "*Add a security exception*".

It is possible to configure cOS Core to use a CA signed certificate instead of self-signed certificate for the management login and doing this is described in the *cOS Core Administration Guide*.

The Login Dialog

cOS Core will next respond like a web server with the initial login dialog page as shown below.



The available Web Interface language options are selectable at the bottom of this dialog. This defaults to the language set for the browser if cOS Core supports that language.

Enter the administrator username **admin** and default password **admin**.

The Setup Wizard

After login, the Web Interface will appear and the cOS Core setup wizard should begin automatically. The first wizard dialog is the wizard welcome screen which should appear as shown below.

Clavister Setup Wizard
Welcome
Welcome to the Clavister Setup Wizard.
The setup wizard will help you to setup:
Administrator user and password.
Time and timezone.
WAN interface configuration.
DHCP server on LAN
(only for models without a pre-configured DHCP Server in the factory configuration).
NTP and syslog server(s).
The wizard can only be completed once, but can be restarted by using the button in the top menu.

Cancelling the Wizard

The setup wizard can be cancelled at any point before the final *Activate* screen and run again by choosing the *Setup Wizard* option from the Web Interface toolbar. Once any configuration changes have been made and activated, either through the wizard, Web Interface or CLI, then the wizard cannot be run since the wizard requires that cOS Core has the factory defaults.

The Wizard Assumes Internet Access will be Configured

The wizard assumes that Internet access will be configured. If this is not the case, for example if

the Clavister Security Gateway is being used in *Transparent Mode* between two internal networks, then the configuration setup is best done with manual Web Interface steps or through the CLI instead of through the wizard and these are explained in the two sections that follow.

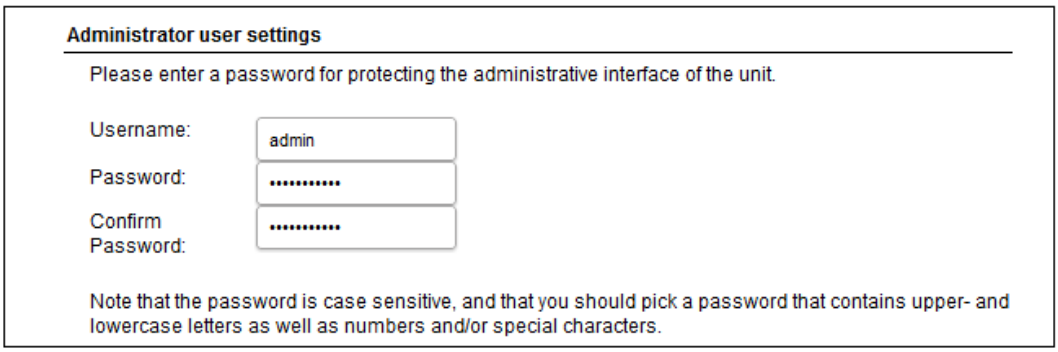
Advantages of the Wizard

The wizard makes setup easier because it automates what would otherwise be a more complex set of individual setup steps. It also reminds you to perform important tasks such as setting the date and time and configuring a log server.

The steps that the wizard goes through after the welcome screen are listed next.

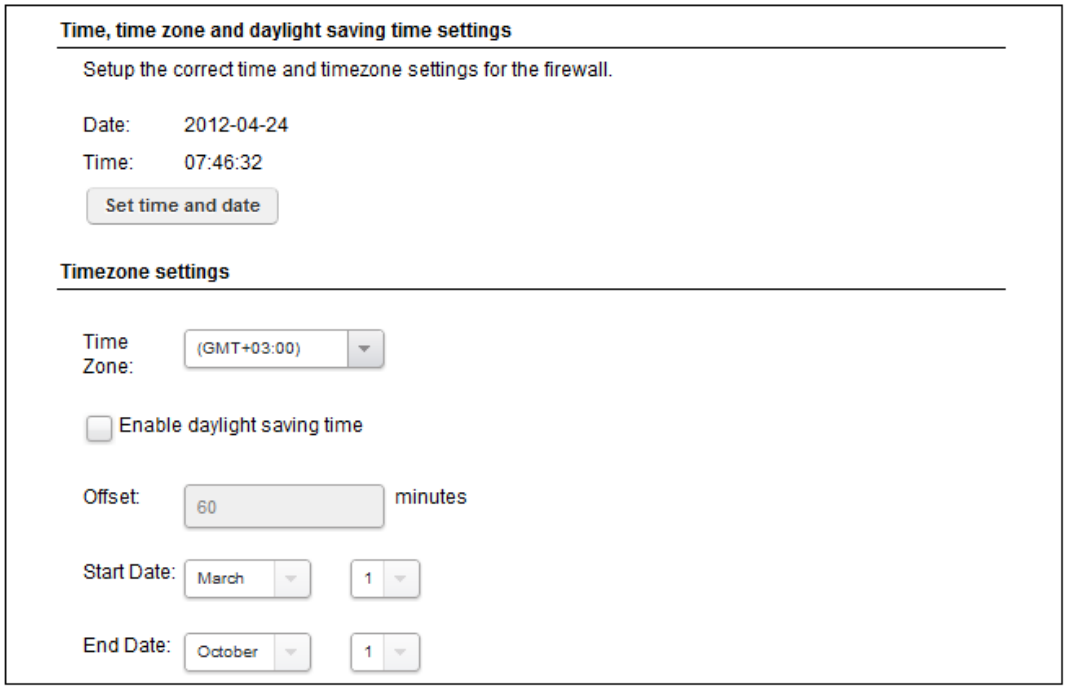
Wizard step 1: Enter a new username and password

You will be prompted to enter a new administration username and password as shown below. It is recommended that this is always done and the new username/password is remembered (if these are forgotten, restoring to factory defaults will restore the original *admin/admin* combination). The password should be composed in a way which makes it difficult to guess.


Administrator user settings
Please enter a password for protecting the administrative interface of the unit.
Username:
admin
Password:
Confirm Password:
Note that the password is case sensitive, and that you should pick a password that contains upper- and lowercase letters as well as numbers and/or special characters.

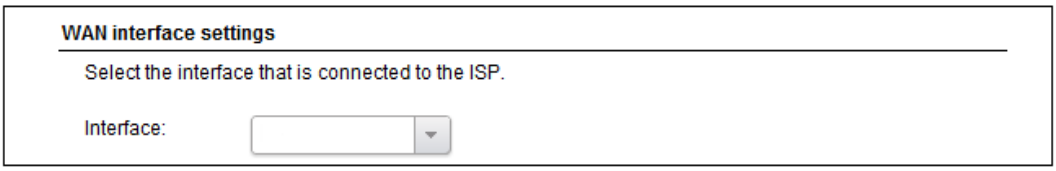
Wizard step 2: Set the date and time

Many cOS Core functions rely on an accurate date and time, so it is important that this is set correctly in the fields shown below.


Time, time zone and daylight saving time settings
Setup the correct time and timezone settings for the firewall.
Date: 2012-04-24
Time: 07:46:32
Set time and date
Timezone settings
Time Zone: (GMT+03:00)
Enable daylight saving time
Offset: 60 minutes
Start Date: March 1
End Date: October 1

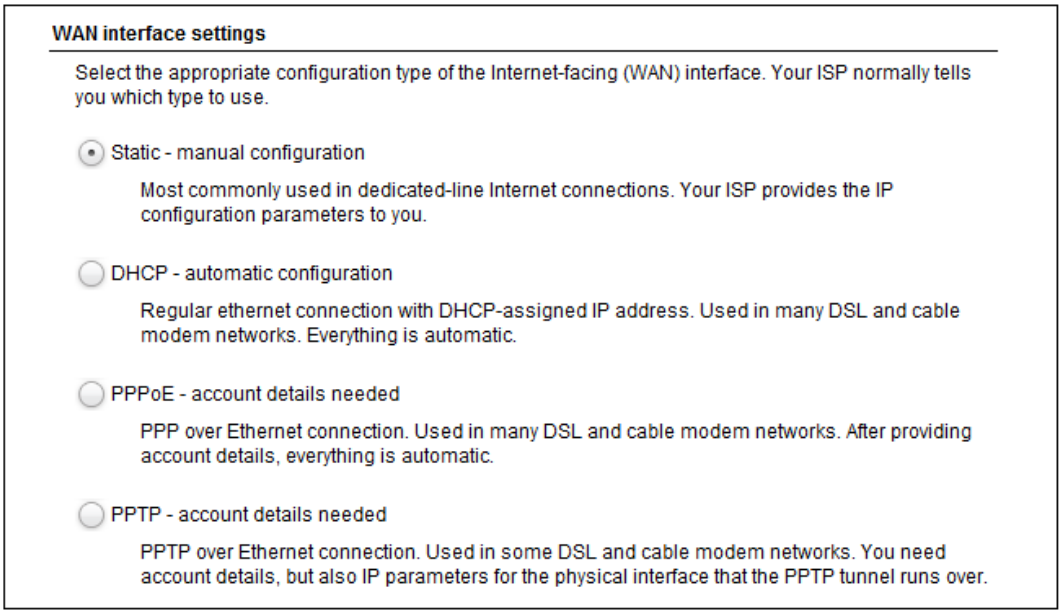
Wizard step 3: Select the *WAN* interface

Next, you will be asked for the *WAN* interface that will be used to connect to an ISP for Internet access.



Wizard step 4: Select the *WAN* interface settings

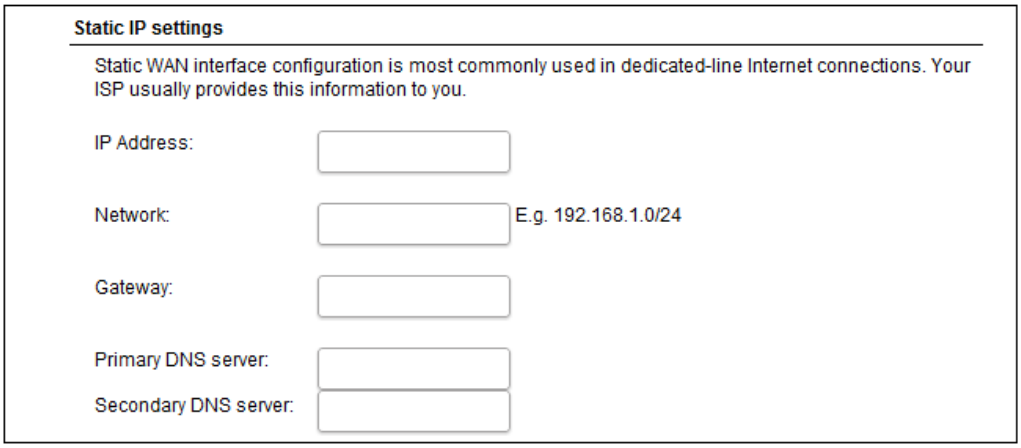
This step selects how the WAN connection to the Internet will function. It can be one of *Manual configuration*, *DHCP*, *PPPoE* or *PPTP* as shown below.


WAN interface settings
Select the appropriate configuration type of the Internet-facing (WAN) interface. Your ISP normally tells you which type to use.
Static - manual configuration
Most commonly used in dedicated-line Internet connections. Your ISP provides the IP configuration parameters to you.
DHCP - automatic configuration
Regular ethernet connection with DHCP-assigned IP address. Used in many DSL and cable modem networks. Everything is automatic.
PPPoE - account details needed
PPP over Ethernet connection. Used in many DSL and cable modem networks. After providing account details, everything is automatic.
PPTP - account details needed
PPTP over Ethernet connection. Used in some DSL and cable modem networks. You need account details, but also IP parameters for the physical interface that the PPTP tunnel runs over.

These four different connection options are discussed next in the subsections **4A** to **4D** that follow.

- **4A. Static - manual configuration**

  Information supplied by the ISP should be entered in the next wizard screen. All fields need to be entered except for the *Secondary DNS server* field.

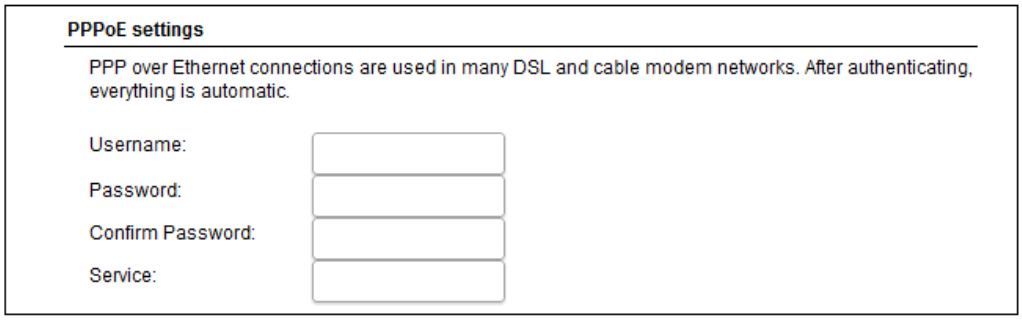

Static IP settings
Static WAN interface configuration is most commonly used in dedicated-line Internet connections. Your ISP usually provides this information to you.
IP Address:
Network:
E.g. 192.168.1.0/24
Gateway:
Primary DNS server:
Secondary DNS server:

- **4B. DHCP - automatic configuration**

  All required IP addresses will automatically be retrieved from the ISP's DHCP server with this option. No further configuration is required for this so it does not have its own wizard screen.

- **4C. PPPoE settings**

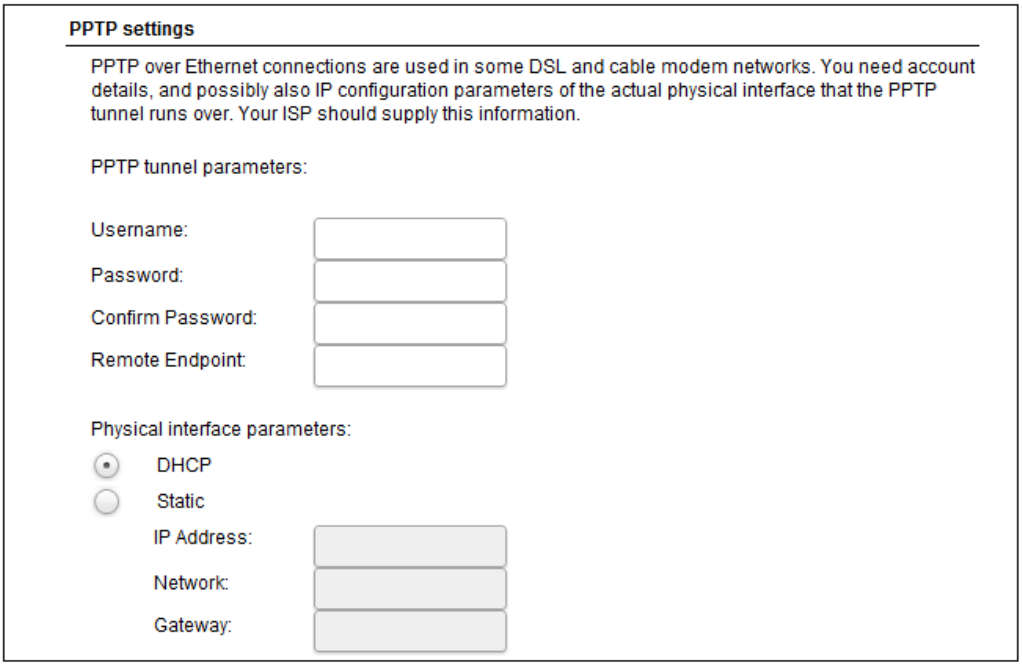
  The username and password supplied by an ISP for PPPoE connection should be entered. The *Service* field should be left blank unless the ISP supplies a value for it.


PPPoE settings
PPP over Ethernet connections are used in many DSL and cable modem networks. After authenticating, everything is automatic.
Username:
Password:
Confirm Password:
Service:

DNS servers are set automatically after connection with PPPoE.

- **4D. PPTP settings**

  The username and password supplied by an ISP for PPTP connection should be entered. If DHCP is to be used with the ISP then this should be selected, otherwise *Static* should be selected followed by entering the static IP address supplied by the ISP.


PPTP settings
PPTP over Ethernet connections are used in some DSL and cable modem networks. You need account details, and possibly also IP configuration parameters of the actual physical interface that the PPTP tunnel runs over. Your ISP should supply this information.
PPTP tunnel parameters:
Username:
Password:
Confirm Password:
Remote Endpoint:
Physical interface parameters:
DHCP
Static
IP Address:
Network:
Gateway:

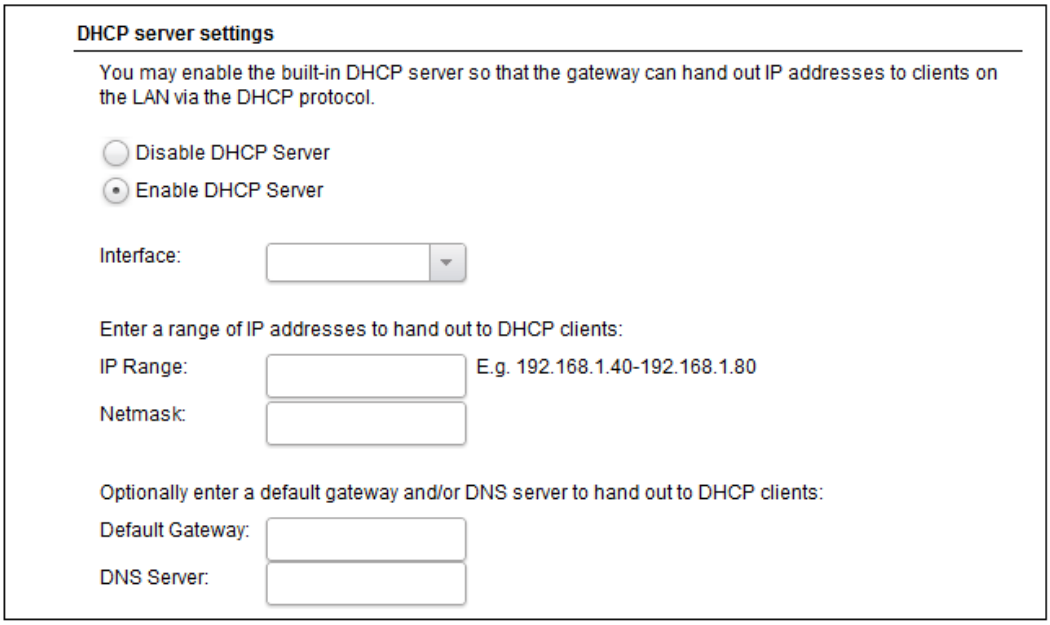
DNS servers are set automatically after connection with PPTP.

Wizard step 5: DHCP server settings

If the Clavister Security Gateway is to function as a DHCP server, it can be enabled here in the wizard on a particular interface or configured later.

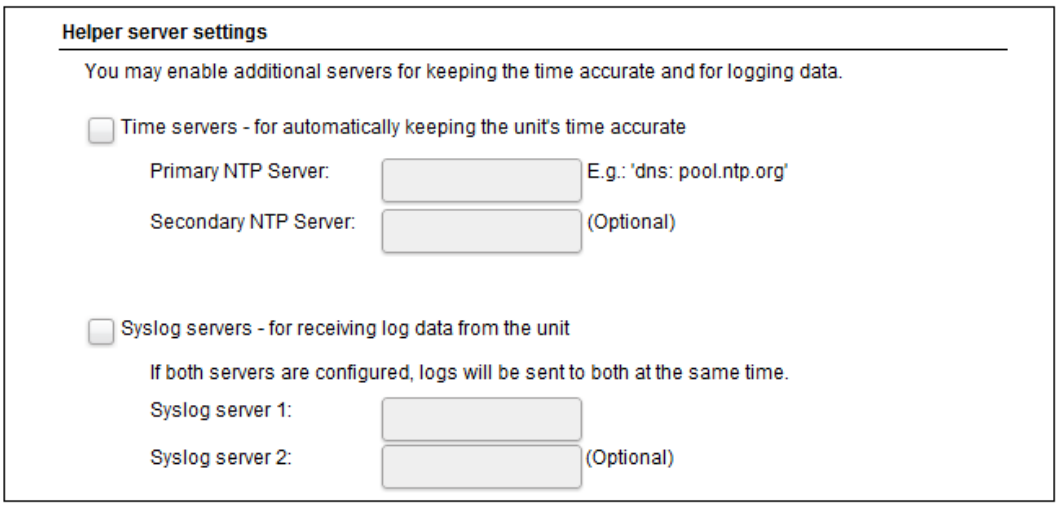
The range of IPv4 addresses that can be handed out must be specified in the form *n.n.n.n - n.n.n.n*, where *n* is a number between 0 and 255 and *n.n.n.n* is a valid IPv4 address within a subnet local to the security gateway.

For example, the private IPv4 address range might be specified as *192.168.1.50 - 192.168.1.150* with a netmask of *255.255.255.0*.


DHCP server settings
You may enable the built-in DHCP server so that the gateway can hand out IP addresses to clients on the LAN via the DHCP protocol.
Disable DHCP Server
Enable DHCP Server
Interface:
Enter a range of IP addresses to hand out to DHCP clients:
IP Range:
E.g. 192.168.1.40-192.168.1.80
Netmask:
Optionally enter a default gateway and/or DNS server to hand out to DHCP clients:
Default Gateway:
DNS Server:

Wizard step 6: Helper server settings

Optional NTP and Syslog servers can be enabled here in the wizard or configured later. *Network Time Protocol* servers keep the system date and time accurate. Syslog servers can be used to receive and store log messages sent by cOS Core.

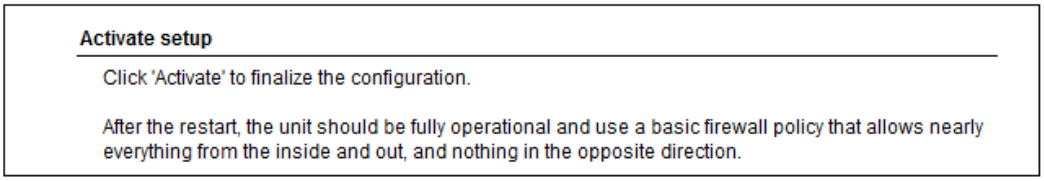

Helper server settings
You may enable additional servers for keeping the time accurate and for logging data.
Time servers - for automatically keeping the unit's time accurate
Primary NTP Server:
E.g.: 'dns: pool.ntp.org'
Secondary NTP Server:
(Optional)
Syslog servers - for receiving log data from the unit
If both servers are configured, logs will be sent to both at the same time.
Syslog server 1:
Syslog server 2:
(Optional)

For the default gateway, it is recommended to specify the IPv4 address assigned to the internal network interface. In this setup, this corresponds to *192.168.1.1*. The DNS server specified should be the DNS supplied by an ISP.

When specifying a hostname as a server instead of an IP address, the hostname should be prefixed with the string *dns:*. For example, the hostname *host1.company.com* should be entered as *dns:host1.company.com*.

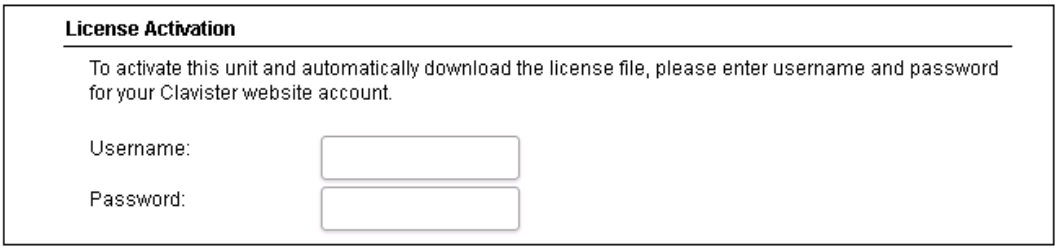
Wizard step 7: Activate setup

The final step for the configuration is to save and activate it by pressing the *Activate* button. After this step the Web Interface returns to its normal appearance and the administrator can continue to configure the system.


Activate setup
Click 'Activate' to finalize the configuration.
After the restart, the unit should be fully operational and use a basic firewall policy that allows nearly everything from the inside and out, and nothing in the opposite direction.

Wizard step 8: License Activation

This optional step is to install a license which is fetched automatically from Clavister servers. Internet access must have been set up in previous wizard steps for this option to function. The only input required is the customer username and password for the Clavister website.


License Activation
To activate this unit and automatically download the license file, please enter username and password for your Clavister website account.
Username:
Password:

If customer registration has not been previously been done, a link is provided to open a browser window to complete registration. After registration, come back to this step.

Alternatively, this step can be skipped and license installation can be done later, in which case cOS Core will run in demo mode with a 2 hour time limit before it ceases to function.

If a license is installed at this point, the wizard will then ask if a reconfigure or restart operation should be performed. If all license parameters are to take effect, the restart option should be chosen. It is recommended to always choose restart unless there is a reason why this is not appropriate.

Running the Wizard Again

Once the wizard has been successfully finished and activated, it cannot be run again. The exception to this is if the Clavister Security Gateway has its factory defaults restored in which case the appliance will behave as though it were being started for the first time.

4.3. Manual Web Interface Setup

This section describes initial cOS Core configuration performed directly through the Web Interface, without using the setup wizard. Configuration is done as a series of individual steps, giving the administrator more direct control over the process. Even if the wizard is used, this section can also be read as a good introduction to using the Web Interface for configuring key aspects of cOS Core.

Ethernet Interfaces

The physical connection of external networks to the Clavister Security Gateway is through the various *Ethernet interfaces* which are provided by the hardware platform. On first-time startup, cOS Core scans for these interfaces and determines which are available and allocates their names. The first interface detected in the scan always becomes the initial default management interface and this cannot be changed beforehand.

All cOS Core interfaces are logically equal for cOS Core and although their physical capabilities may be different, any interface can perform any logical function. With the E7, the **GESW** interface is the default management interface. The other interfaces can be used as required. For this section, it is assumed that the **G2** interface will be used for connection to the public Internet and the **G3** interface will be used for connection to a protected, local network.

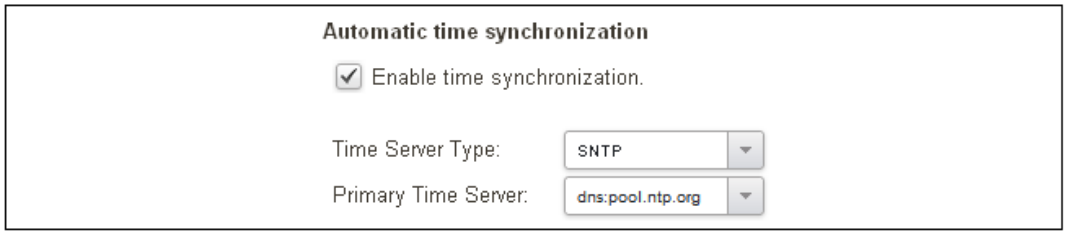
Setting the Date and Time

Many cOS Core functions rely on an accurate date and time, so it is important that this is set correctly. To do this, select **System > Device > Date and Time**.

Date and Time
Set the date, time and time zone information for this system.
General
Current Date and Time: 2012-04-16 14:16:53
Set Date and Time

By pressing the **Set Date and Time** button, a dialog appears that allows the exact time to be set.

A **Network Time Protocol** (NTP) servers can optionally be configured to maintain the accuracy of the system date and time and this will require public Internet access. Enabling this option is strongly recommended since it ensures the accuracy of the date and time. A typical NTP setup is shown below.



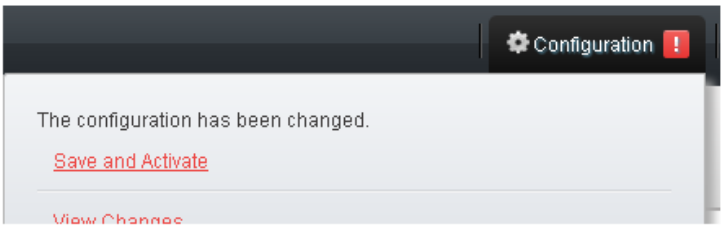
Important: The time server URL requires the "dns:" prefix

*When specifying a URL in cOS Core for the time server, it **must** have the prefix "**dns:**".*

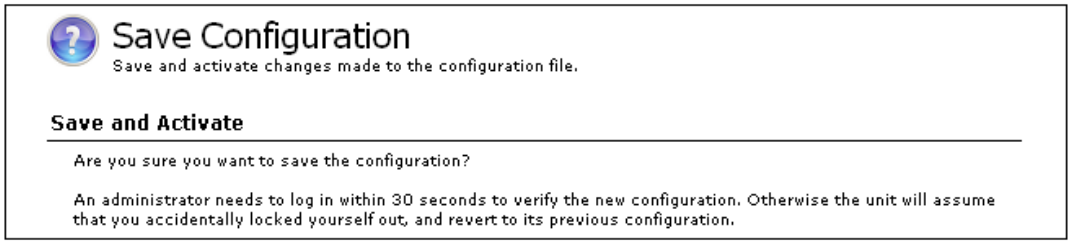
Once the values are set correctly, we can press the **OK** button to save the values while we move on to more steps in cOS Core configuration. Although changed values like this are saved by cOS Core, they do not become active until the entire saved configuration becomes the current and active configuration. We will look at how to do this next.

Activating Configuration Changes

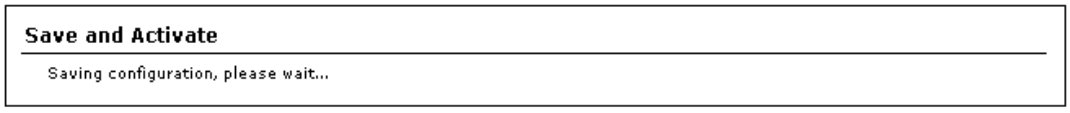
To activate any cOS Core configuration changes made so far, select the **Save and Activate** option from the **Configuration** menu (this procedure is also referred to as *deploying* a configuration).



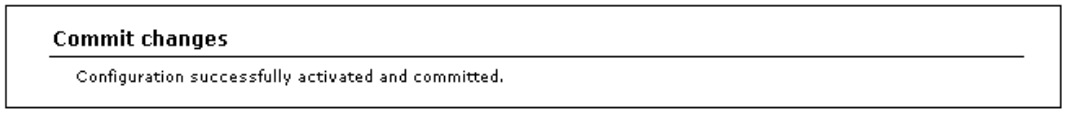
A dialog is then presented to confirm that the new configuration is to become the running configuration.


Save Configuration
Save and activate changes made to the configuration file.
Save and Activate
Are you sure you want to save the configuration?
An administrator needs to log in within 30 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.

After clicking **OK**, cOS Core *reconfiguration* will take place and, after a short delay, the Web Interface will try and connect again to the security gateway.



If no reconnection is detected by cOS Core within 30 seconds (this length of time is a setting that can be changed) then cOS Core will revert back to the original configuration. This is to ensure that the new configuration does not accidentally lock out the administrator. After reconfiguration and successful reconnection, a success message is displayed indicating successful reconfiguration.



Reconfiguration is a process that the cOS Core administrator may initiate often. Normally, reconfiguration takes a brief amount of time and causes only a slight delay in traffic throughput. Active user connections through the Clavister Security Gateway should rarely be lost.

Tip: How frequently to commit configuration changes

It is up to the administrator to decide how many changes to make before activating a new configuration. Sometimes, activating configuration changes in small batches can be appropriate in order to check that a small set of changes work as planned.

However, it is not advisable to leave changes uncommitted for long periods of time, such as overnight, since any system outage will result in these edits being lost.

Automatic Logout

If there is no activity through the Web Interface for a period of time (the default is 15 minutes), cOS Core will automatically log the user out. If they log back in through the same web browser session then they will return to the point they were at before the logout occurred and no saved (but not yet activated) changes are lost.

Setting Up Internet Access

Next, we shall look at how to set up public Internet access. The setup wizard described in the previous chapter, provides the following four options:

A. Static - manual configuration.

B. DHCP - automatic configuration.

C. PPPoE setup

D. PPTP setup

The individual manual steps to configure these connection alternatives with the Web Interface are discussed next.

A. Static - manual configuration

Manual configuration means that there will be a direct connection to the ISP and all the relevant IP addresses for the connecting interface are fixed values provided by the ISP which are entered into cOS Core manually.

Note: The interface DHCP option should be disabled

For static configuration of the Internet connection, the DHCP option must be disabled (the default) in the properties of the interface that will connect to the ISP.

The initial step is to set up a number of IPv4 address objects in the cOS Core *Address Book*. Let us assume for this section that the interface used for Internet connection is **G2** and that the static IPv4 address for this interface is to be *10.5.4.35*, the ISP's gateway IPv4 address is *10.5.4.1*, and the network to which they both belong is *10.5.4.0/24*.

Note: Private IPv4 addresses are used for example only

Each installation's IP addresses will be different from the IP addresses used here in the examples. Also, the addresses used in the examples are private IPv4 addresses and in reality an ISP would issue public IPv4 addresses for Internet access.

Now, add the gateway *IP4 Address* object using the address book name *wan_gw* and assign it the IPv4 address *10.5.4.1*. The ISP's gateway is the first router hop towards the public Internet from the Clavister Security Gateway. Go to **Objects > Address Book** in the Web Interface.

The current contents of the address book will be listed and will contain a number of predefined objects created by cOS Core after it scans the interfaces for the first time. The screenshot below shows the initial address book for the E7.

#	Name	Address	User Auth Groups	Comments
1	InterfaceAddresses			
2	all-nets	0.0.0.0/0		All possible networks
3	localhost	127.0.0.1 (127.0.0.2)		Localhost, for non-management High Availabilit
4	all-nets6	::/0		All possible IPv6 networks

Note: The all-nets address

*The IPv4 address object **all-nets** is a wildcard address that should never be changed and can be used in many types of cOS Core rules to refer to any IPv4 address or network range.*

For the E7, all the Ethernet interface related address objects are gathered together in an *address book folder* called *InterfaceAddresses*. By clicking on this folder, it will be opened and the individual address objects it contains can be viewed. The first few default addresses in the folder are shown below.

#	Name	Address	User Auth Groups	Comments
1	G1_ip	192.168.1.1		IP address of interface G1
2	G2_ip	127.0.1.1		IP address of interface G2
3	G3_ip	127.0.2.1		IP address of interface G3
4	G4_ip	127.0.3.1		IP address of interface G4
5	G1_net	192.168.1.0/24		Network on interface G1
6	G2_net	127.0.1.0/24		Network on interface G2

On initial startup, two IPv4 address objects are created automatically for each interface detected by cOS Core. One IPv4 address object is named by combining the physical interface name with the suffix "*_ip*" and this is used for the IPv4 address assigned to that interface. The other address

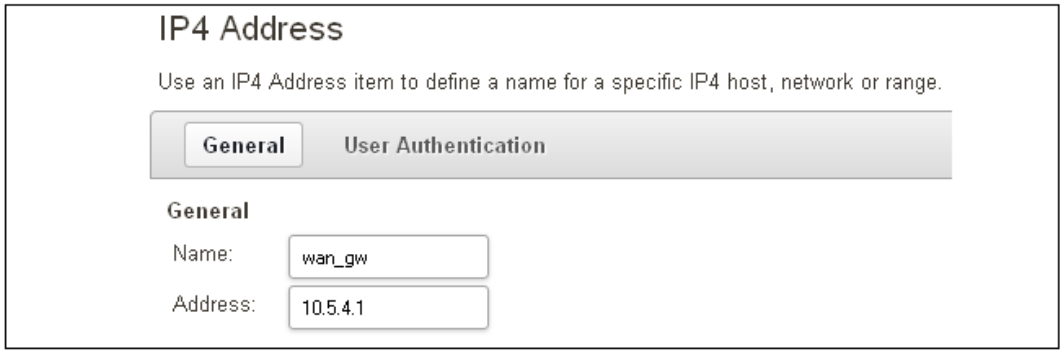
object is named by combining the interface name with the suffix "*_net*" and this is the network to which the interface belongs.

Tip: Creating address book folders

New folders can be created when needed and provide a convenient way to group together related IP address objects. The folder name can be chosen to indicate the folder's contents.

Now click the **Add** button at the top left of the list and choose the *IP4 Address* option to add a new address to the folder.

Enter the details of the object into the properties fields for the *IP4 Address* object. Below, the IPv4 address *10.5.4.1* has been entered for the address object called *wan_gw*. This is the IP of the ISP's router which acts as the gateway to the public Internet.



Click the **OK** button to save the values entered.

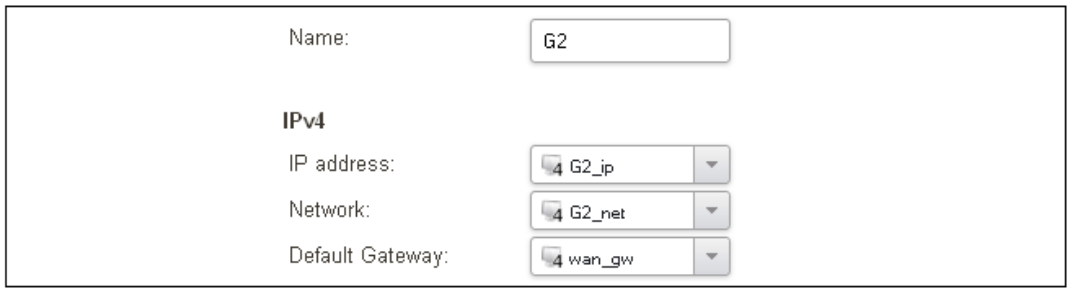
Then set up *G2_ip* to be *10.5.4.35*. This is the IPv4 address of the **G2** interface which will connect to the ISP's gateway.

Lastly, set the *IP4 Address* object *G2_net* to be *10.5.4.0/24*. Both *G2_ip* and *wan_gw* must belong to this network in order for the interface to communicate with the ISP.

Together, these three IPv4 address objects will be used to configure the interface connected to the Internet which in this example is **G2**. Select **Network > Interfaces and VPN > Ethernet** to display a list of the physical interfaces. The first lines of the interface list for the E7 are shown below.

#	Name	IPv4 Address	IPv6 Address	Network	Default Gateway	Enable DHCP Client	Comment
1	G1	G1_ip		G1_net		No	
2	G2	G2_ip		G2_net		No	
3	G3	G3_ip		G3_net		No	

Click on the interface in the list which is to be connected to the Internet. The properties for this interface will now appear and the settings can be changed including the default gateway.



Press **OK** to save the changes. Although changes are remembered by cOS Core, the changed configuration is not yet activated and won't be activated until cOS Core is told explicitly to use the changed configuration.

Remember that DHCP should **not** be enabled when using static IP addresses and also that the IP address of the *Default Gateway* (which is the ISP's router) **must** be specified. As explained in more detail later, specifying the *Default Gateway* also has the additional effect of automatically adding a route for the gateway in the cOS Core routing table.

At this point, the connection to the Internet is configured but no traffic can flow to or from the Internet since all traffic needs a minimum of the following two cOS Core configuration objects to exist before it can flow through the Clavister Security Gateway:

- An *IP rule* or *IP Policy* object that explicitly allows traffic to flow from a given source network and source interface to a given destination network and destination interface.
- A *route* defined in a cOS Core routing table which specifies on which interface cOS Core can find the traffic's destination IP address.

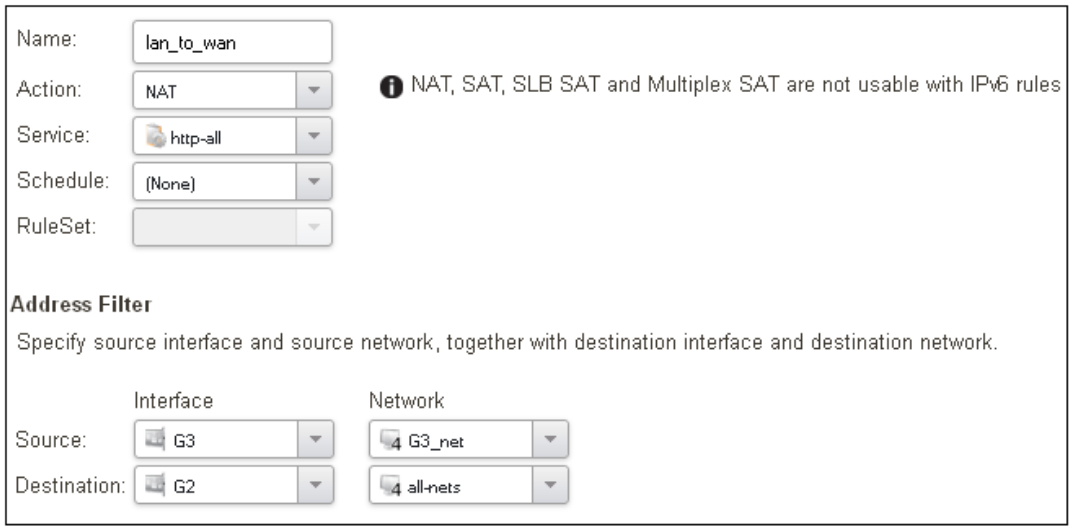
  If multiple matching routes are found, cOS Core uses the route that has the smallest (in other words, the narrowest) IP range.

We must therefore first define an IP rule that will allow through traffic from a designated source interface and source network. In this case let us assume we want to allow web browsing from the internal network *G3_net* connected to the interface **G3** to be able to access the public Internet.

To do this, first go to **Policies > Firewalling > Main IP Rules**.

The empty *main* IP rule set will now appear. Press the **Add** button at the top left and select **IP Rule** from the menu.

The properties for the new IP rule will appear. In this example, we will call the rule *lan_to_wan*. The rule *Action* is set to *NAT* (this is explained further below) and the *Service* is set to *http-all* which is suitable for most web browsing (it allows both HTTP and HTTPS connections). The interface and network for the source and destinations are defined in the *Address Filter* section of the rule.



The destination network in the IP rule is specified as the predefined *IP4 Address* object *all-nets*. This is used since it cannot be known in advance to which IP address web browsing will be directed and *all-nets* allows browsing to any IP address. IP rules are processed in a top down fashion, with the search ending at first matching rule. An *all-nets* rule like this should be placed towards the bottom or at the end of the rule set since other rules with narrower destination addresses should trigger before it does.

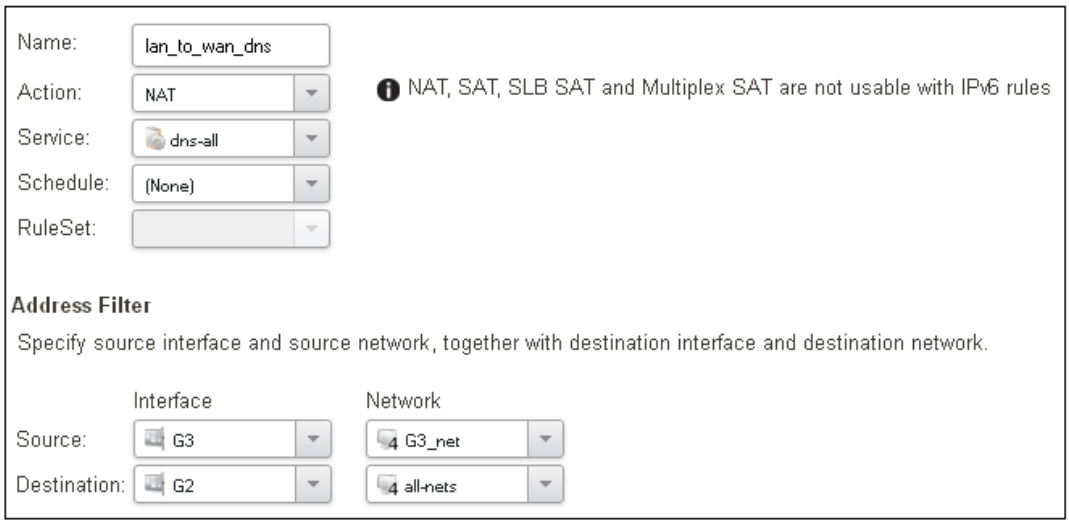
Only one rule is needed since any traffic controlled by a *NAT* rule will be controlled by the cOS Core *state engine*. This means that the rule will allow *connections* that originate from the source network/destination and also implicitly allow any returning traffic that results from those connections.

In the above, the predefined service called *http-all* is the best service to use for web browsing (this service includes HTTP and HTTPS but not DNS). It is advisable to always make the service in an IP rule or IP policy as restrictive as possible to provide the best security possible. Custom service objects can be created for specific protocols and existing service objects can also be combined into a new, single service object.

The IP rule *Action* could have been specified as *Allow*, but only if all the hosts on the protected local network have public IPv4 addresses. By using *NAT*, cOS Core will use the destination interface's IP address as the source IP. This means that external hosts will send their responses back to the interface IP and cOS Core will automatically forward the traffic back to the originating local host. Only the outgoing interface therefore needs to have a public IPv4 address and the internal network topology is hidden.

To allow web browsing, DNS lookup also needs to be allowed in order to resolve URLs into IP addresses. The service *http-all* does not include the *DNS* protocol so a similar IP rule that allows

this is needed. This could be done with a single IP rule or IP policy that uses a custom service which combines the *HTTP* and *DNS* protocols but the recommended method is to create an entirely new IP rule that mirrors the above rule but specifies the service as *dns-all*. This method provides the most clarity when the configuration is examined for any problems. The screenshot below shows a new IP rule called *lan_to_wan_dns* being created to allow DNS.



Like the IP rule for HTTP, this rule also specifies that the action for DNS requests is *NAT* so all DNS request traffic is sent out by cOS Core with the outgoing interface's IP address as the source IP.

For the Internet connection to work, a *route* also needs to be defined so that cOS Core knows on which interface the web browsing traffic should leave the Clavister Security Gateway. This route will define the interface where the network *all-nets* (in other words, any network) will be found. If the default *main* routing table is opened by going to **Network > Routing > Routing Tables > main**, the route needed should appear as shown below.

Type	Interface	Network	Gateway	LocalIP	Metric	Monitor this route	Comments
Route IPv4	G2	all-nets	wan_gw		100	No	

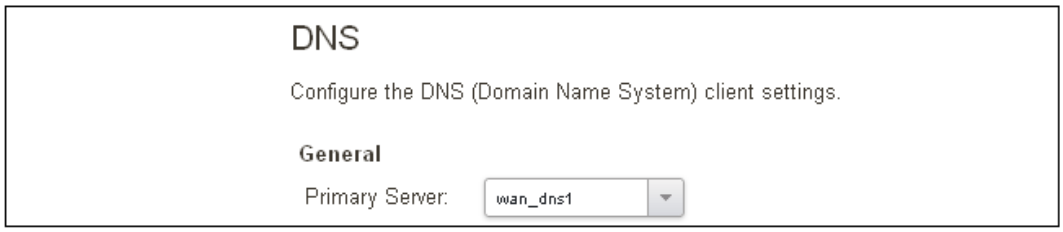
This required *all-nets* route is, in fact, added automatically after specifying the *Default Gateway* for a particular Ethernet interface and this was done earlier when setting up the required *IP4 Address* objects.

Note: Disabling automatic route generation

*Automatic route generation is enabled and disabled with the setting "**Automatically add a default route for this interface using the given default gateway**" which can be found in the properties of the interface.*

As part of the setup, it is also recommended that at least one DNS server is also defined in cOS Core. This DSN server or servers (a maximum of three can be configured) will be used when cOS Core itself needs to resolve URLs which is the case when a URL is specified in a configuration object instead of an IP address. It is also important for certificate handling

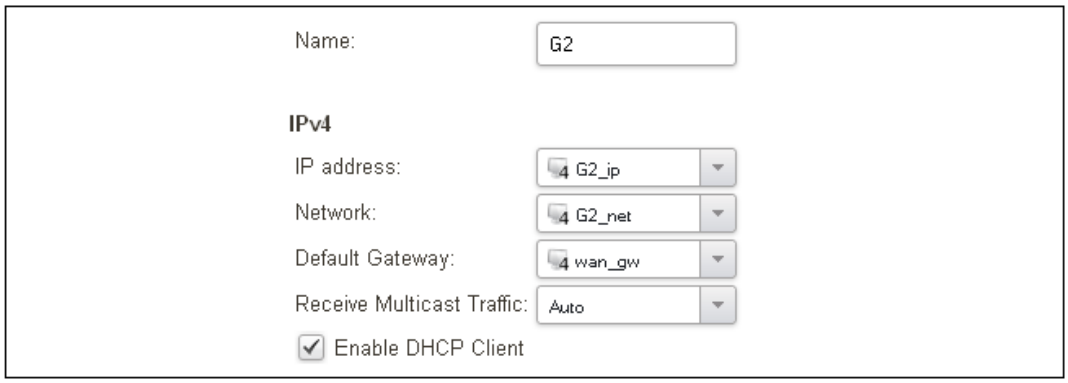
Let's assume an IPv4 address object called *wan_dns1* has already been defined in the address book and this is the address for the first DNS server. By choosing **System > Device > DNS**, the DNS server dialog will open and this object from the address book can be assigned as the first server.



B. DHCP - automatic configuration

All the required IP addresses for Internet connection can, alternatively, be automatically retrieved from an ISP's DHCP server by enabling the **DHCP Client** option for the interface connected to the ISP. This option is enabled by first selecting **Network > Interfaces and VPN > Ethernet** to display a list of all the interfaces.

Click the **G2** interface in the list to display its properties and select the option to enable the interface as a DHCP client.



Usually, a DHCP *Host Name* does not need to be specified but can sometimes be used by an ISP to uniquely identify this Clavister Security Gateway as a particular DHCP client to the ISP's DHCP server.

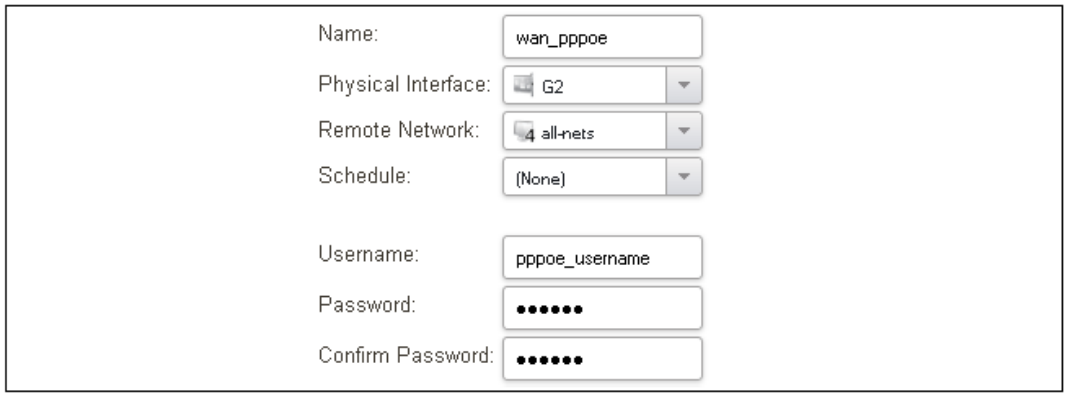
On connection to the ISP, all required IP addresses are retrieved automatically from the ISP via DHCP and cOS Core automatically sets the relevant address objects in the address book with this information.

For cOS Core to know on which interface to find the public Internet, a *route* has to be added to the *main* cOS Core routing table which specifies that the network *all-nets* can be found on the interface connected to the ISP and this route must also have the correct *Default Gateway* IP address specified. This *all-nets* route is added automatically by cOS Core during the DHCP address retrieval process.

After all IP addresses are set via DHCP and an *all-nets* route is added, the connection to the Internet is configured but no traffic can flow to or from the Internet since there is no IP rule defined that allows it. As was done in the previous option (**A**) above, we must therefore define an IP rule that will allow traffic from a designated source interface and source network. (in this example, the network *G3_net* and interface **G3**) to flow to the destination network *all-nets* and the destination interface **G2**.

C. PPPoE setup

For PPPoE connection, we must create a PPPoE tunnel interface associated with the physical Ethernet interface. Assume that the physical interface is **G2** and the PPPoE tunnel object created is called *wan_pppoe*. Go to **Network > Interfaces and VPN > PPPoE** and select **Add > PPPoE Tunnel**. These values can now be entered into the PPPoE Tunnel properties dialog.



An ISP will supply the correct values for *pppoe_username* and *pppoe_password* in the dialog above.

The PPPoE tunnel interface can now be treated exactly like a physical interface by the policies defined in cOS Core rule sets.

There also has to be a route associated with the PPPoE tunnel to allow traffic to flow through it, and this is automatically created in the *main* routing table when the tunnel is defined. If we go to **Network > Routing > Routing Tables > main** we can see this route.

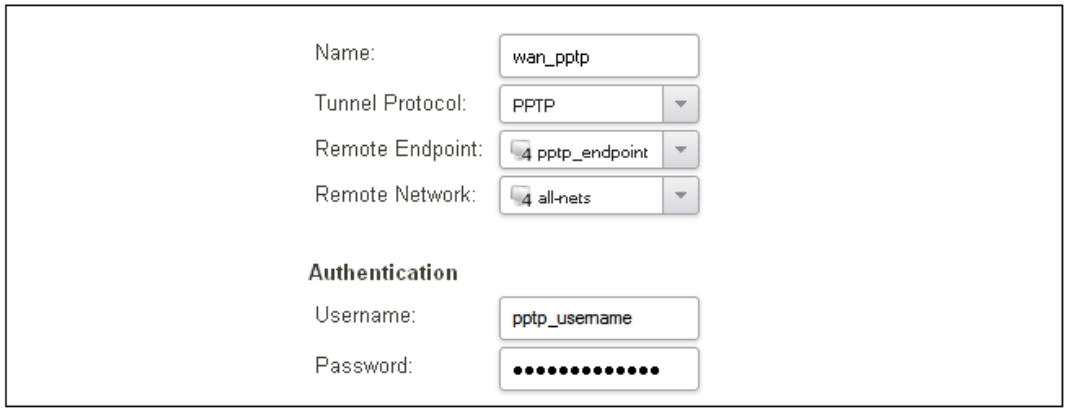
Type	Interface	Networ...	Gateway	LocalIP	Metric	Monitor this route
Route IPv4	wan_pppoe	all-nets			90	No

If the PPPoE tunnel object is deleted, this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source interface and source network (in this example, the network *G3_net* and interface **G3**) to flow to the destination network *all-nets* and the destination interface which is the PPPoE tunnel that has been defined.

D. PPTP setup

For PPTP connections, a PPTP client tunnel interface object needs to be created. Let us assume that the PPTP tunnel will be called *wan_pptp* with a remote endpoint *10.5.4.1* which has been defined as the *IP4 Address* object *pptp_endpoint*. Go to **Network > Interfaces and VPN > PPTP/L2TP Clients** and select **Add > PPTP/L2TP Client**. The values can now be entered into the properties dialog and the *PPTP* option should be selected.



An ISP will supply the correct values for *pptp_username*, *pptp_password* and the remote endpoint. An interface is not specified when defining the tunnel because this is determined by cOS Core looking up the *Remote Endpoint* IP address in its routing tables.

The PPTP client tunnel interface can now be treated exactly like a physical interface by the policies defined in cOS Core rule sets.

There also has to be an associated route with the PPTP tunnel to allow traffic to flow through it, and this is automatically created in the *main* routing table when the tunnel is defined. The destination network for this route is the *Remote Network* specified for the tunnel and for the public Internet this should be *all-nets*.

If we go to **Network > Routing > Routing Tables > main** we can see this route.

Type	Interface	Network	Gateway	LocalIP	Metric	*Monitor this route*	Comments
Route IPv4	wan_pptp	all-nets			90	No	Direct route for network

If the PPTP tunnel object is deleted, this route is also automatically deleted.

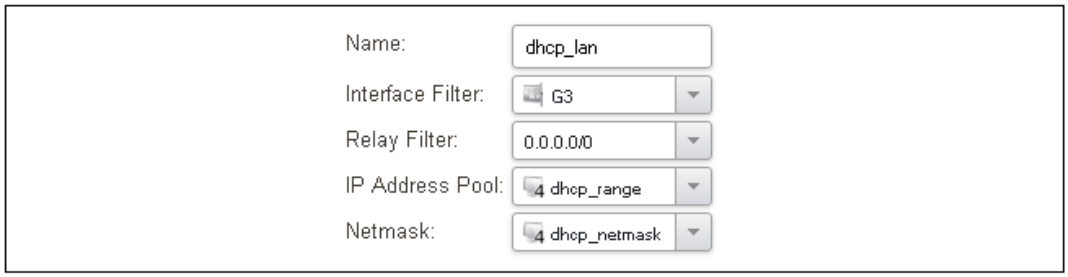
At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source network and source interface (in this example, the network *G3_net* and interface **G3**) to flow to the destination network *all-nets* and the destination interface which is the PPTP tunnel that has been defined.

DHCP Server Setup

If the Clavister Security Gateway is to act as a DHCP server then this can be set up in the following way:

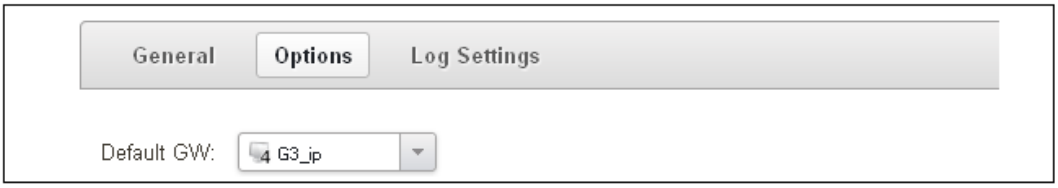
First, create an *IP4 Address* object which defines the address range to be handed out. Here, it is assumed that this has the name *dhcp_range*. It is also assumed that another *IP4 Address* object *dhcp_netmask* has been created which specifies the netmask.

We now create a DHCP server object called *dhcp_lan* which will only be available only on the **G3** interface. To do this, go to **Network > Network Services > DHCP Servers** and select **Add > DHCP Server**. The server properties can now be specified.



An example IP pool range might be *196.168.1.10 - 192.168.1.20* with a netmask of *255.255.0.0*.

In addition, it is important to specify the *Default gateway* for the server. This will be handed out to DHCP clients on the internal networks so that they know where to find the public Internet. The default gateway is always the IPv4 address of the interface on which the DHCP server is configured, in this case, *G3_ip*. Select the **Options** tab to set this.

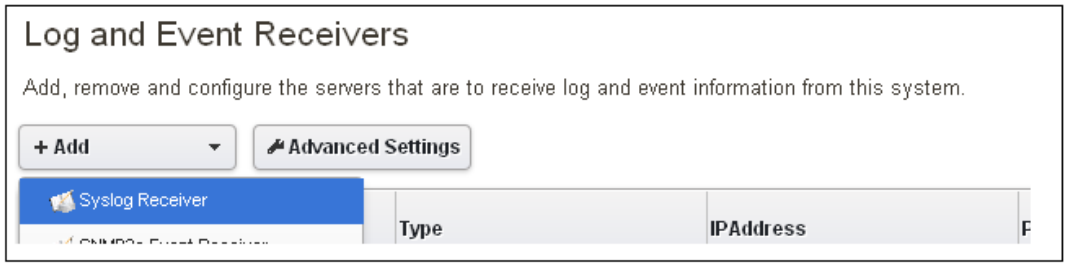


Also in the **Options** tab, we should specify the DNS address which is handed out with DHCP leases. This could be set, for example, to be the IPv4 address object *dns1_address*.

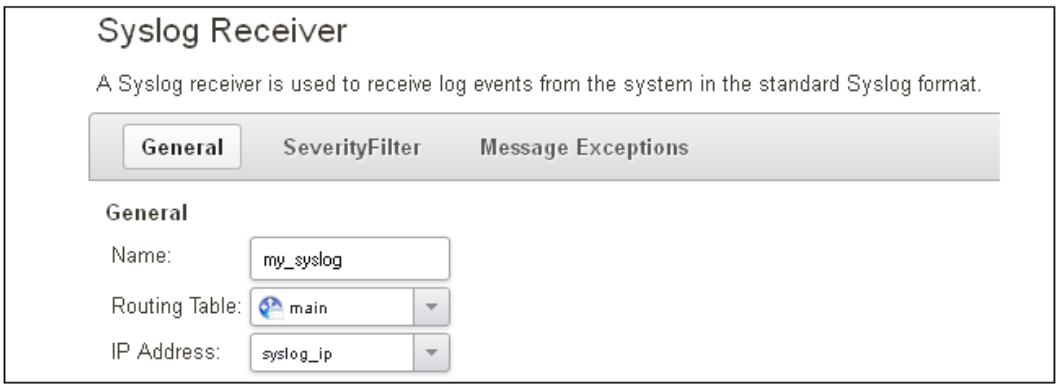
Syslog Server Setup

Although logging may be enabled, no log messages are captured unless at least one log server is set up to receive them and this is configured in cOS Core. *Syslog* is one of the most common server types.

First we create an *IP4 Address* object called, for example, *syslog_ip* which is set to the IPv4 address of the server. We then configure the sending of log messages to a Syslog server from cOS Core by selecting **System > Device > Log and Event Receivers** and then choosing **Add > Syslog Receiver**.


Log and Event Receivers
Add, remove and configure the servers that are to receive log and event information from this system.
+ Add
Advanced Settings
Syslog Receiver
Type
IPAddress

The syslog server properties dialog will now appear. We give the server a name, for example *my_syslog*, and specify its IPv4 address as the *syslog_ip* object.



Tip: Address book object naming

The cOS Core address book is organized alphabetically so when choosing names for IP address objects it is best to have the descriptive part of the name first. In this case, use ***syslog_ip*** *as the name and not* ***ip_syslog****.*

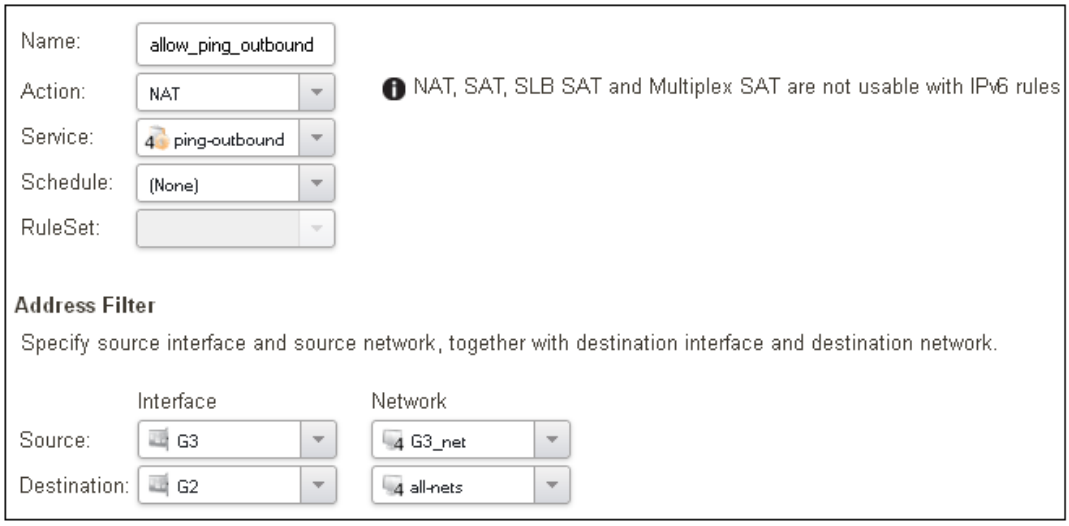
Allowing ICMP *Ping* Requests

As a further example of setting up IP rules, it can be very useful to allow ICMP *Ping* requests to flow through the Clavister Security Gateway. As discussed earlier, the cOS Core will drop any traffic unless an IP rule explicitly allows it. Let us suppose that we wish to allow the pinging of external hosts with the ICMP protocol by computers on the internal *G3_net* network.

There can be several rule sets defined in cOS Core but there is only one rule set defined by default and this is called *main*. To add a rule to it, first select **Policies > Firewalling > Main IP Rules**.

The *main* rule set list contents are now displayed. Press the **Add** button and select **IP Rule**.

The properties for a new IP rule will appear and we can add a rule, in this case called *allow_ping_outbound*.



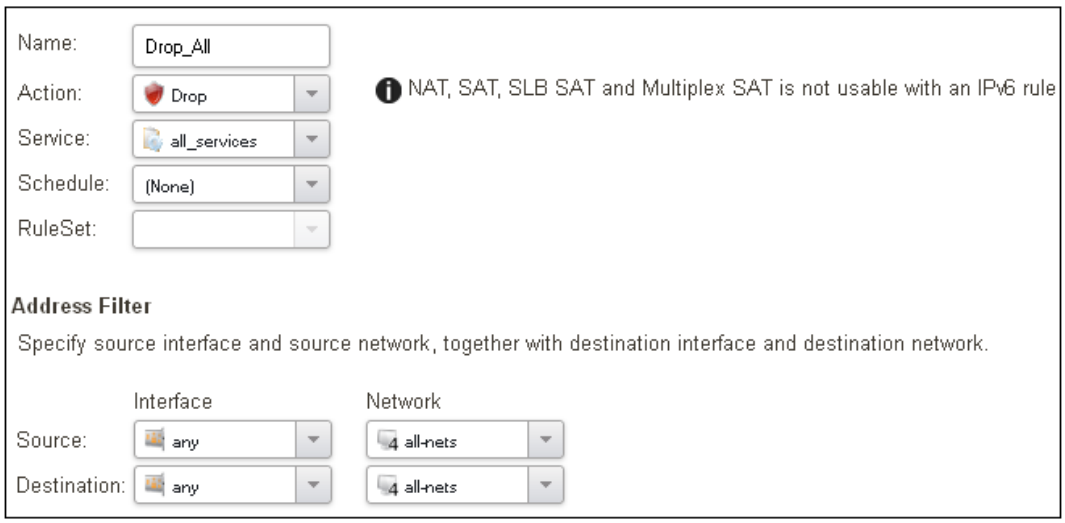
The IP rule again has the *NAT* action and this is necessary if the protected local hosts have private IPv4 addresses. The ICMP requests will be sent out from the Clavister Security Gateway with the IP address of the interface connected to the ISP as the source interface. Responding hosts will send back ICMP responses to this single IP and cOS Core will then forward the response to the correct private IPv4 address.

Adding a Drop All Rule

The top-down nature of the IP rule set scanning has already been discussed earlier. If **no** matching IP rule is found for a new connection then the *default rule* is triggered. This rule is hidden and cannot be changed and its action is to drop all such traffic as well as generate a log message for the drop.

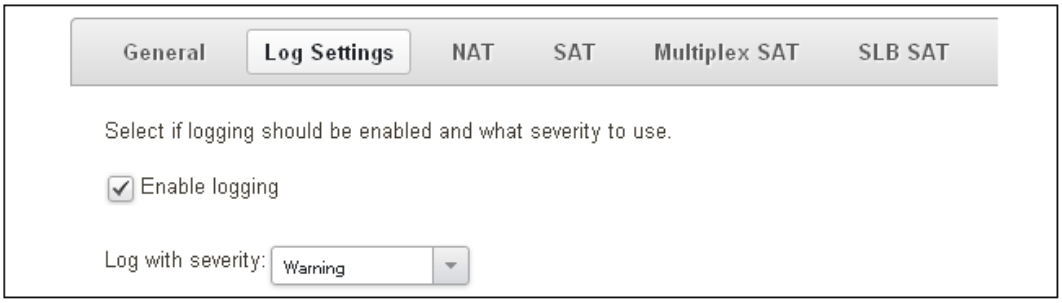
In order to gain control over the logging of dropped traffic, it is recommended to create a drop all rule as the last rule in the *main* IP rule set. This rule has an *Action* of *Drop* with the source and destination network set to *all-nets* and the source and destination interface set to *any*.

The service for this rule must also be specified and this should be set to *all_services* in order to capture all types of traffic.



If the this rule us the only one defined, displaying the *main* IP rule set will be as shown below.

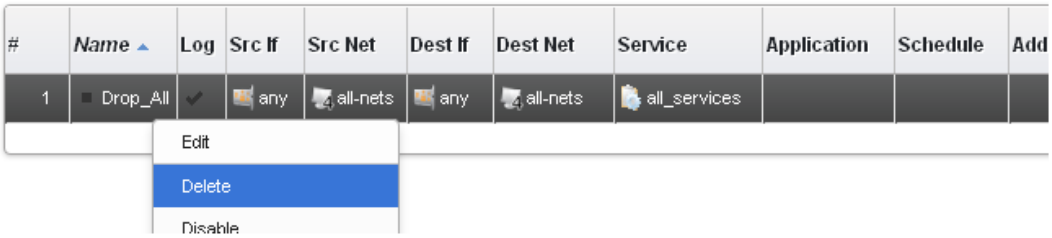
Logging can now be enabled on this rule with the desired severity. Click the **Log Settings** tab, and click the **Enable logging** box. All log messages generated by this rule will be given the selected severity and which will appear in the text of the log messages. It is up to the administrator to choose the severity and depends on how they would like to classify the messages.



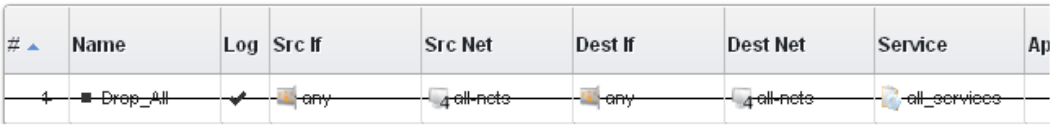
Deleting Configuration Objects

If information is deleted from a configuration during editing then these deletes are indicated by a line scored through the list entry while the configuration is still not yet activated. The deleted entry only disappears completely when the changes are activated.

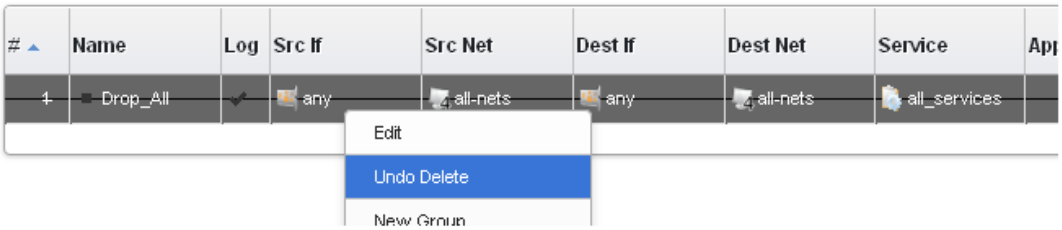
For example, we can delete the drop all IP rule created in the previous paragraph by right clicking the rule and selecting *Delete* in the context menu.



The rule now appears with a line scored through it.



We can reverse the delete by right clicking the rule again and choosing *Undo Delete*.



A valid license should now be installed to remove the cOS Core 2 hour demo mode limitation.

Doing this is described in *Section 4.5, "License Installation Methods"*.

4.4. CLI Setup

This chapter describes the setup steps using CLI commands instead of the setup wizard.

The CLI is accessible using either one of two methods:

- Using an SSH (Secure Shell) client, across a network connection to the IPv4 address *192.168.1.1* on the default management Ethernet interface. The physical network connection setup to the computer running the client is described in *Section 4.1, "Management Workstation Connection"* and is the same as that used in *Section 4.2, "Web Interface and Wizard Setup"*.

  If there is a problem with the workstation connection, a help checklist can be found in *Section 4.6, "Setup Troubleshooting "*.

- Using a terminal or computer running a console emulator connected directly to the local console port on the E7.

The CLI commands listed below are grouped so that they mirror the options available in the setup wizard.

Confirming the Connection

Once connection is made to the CLI, pressing the **Enter** key will cause cOS Core to respond. The response will be a normal CLI prompt if connecting directly through the local console port and a username/password combination will not be required (a password for this console can be set later).

```
Device:/>
```

If connecting remotely through an SSH (Secure Shell) client, an administration username/password must first be entered and the initial default values for these are username *admin* and password *admin*. When these are accepted by cOS Core, a normal CLI prompt will appear and CLI commands can be entered.

Changing the Password

To change the administration username or password, use the *set* command to change the current CLI object category (also referred to as the *context*) to be the *LocalUserDatabase* called *AdminUsers*.

```
Device:/> cc LocalUserDatabase AdminUsers
Device:/AdminUsers>
```

Tip: Using tab completion with the CLI

The tab key can be pressed at any time so that cOS Core gives a list of possible options in a command.

Now set the username and password for the administrator. Both are case sensitive. In the example below, the username is set to the value *new_name* and the password is set to the value *new_pass*.

```
Device:/AdminUsers> set User Admin Name=new_name Password=new_pass
```

The new username/password combination should be remembered and the password should be composed in a way which makes it difficult to guess. The next step is to return the CLI to the default context which is the top level of object categories.

```
Device:/AdminUsers> cc
Device:/>
```

Setting the Date and Time

Many cOS Core functions, such as event logging and certificate handling, rely on an accurate date and time. It is therefore important that this is set correctly using the *time* command. A typical usage of this command might be:

```
Device:/> time -set 2008-06-24 14:43:00
```

Notice that the date is entered in *yyyy-mm-dd* format and the time is stated in 24 hour *hh:mm:ss* format.

Ethernet Interfaces

The connection of external networks to the Clavister Security Gateway is via the various *Ethernet interfaces* which are provided by the hardware platform. On first-time startup, cOS Core scans for these interfaces and determines which are available and allocates their names. The first interface detected in the scan becomes the initial default management interface and this can only be changed after initial startup.

All cOS Core interfaces are logically equal for cOS Core and although their physical capabilities may be different, any interface can perform any logical function. With the E7, any of the **GESW** interfaces can act as the default management interface. The other interfaces can be used as desired. For the sake of example, it is assumed here that the **G2** interface will be used for connection to the public Internet and the **G3** interface will be used for connection to a protected, local network.

Setting Up Internet Access

Next, we shall look at how to set up public Internet access with the CLI. The setup wizard described previously, provides the following four options:

A. Static - manual configuration.

B. DHCP - automatic configuration.

C. PPPoE setup.

D. PPTP setup.

The individual manual steps to configure these connection alternatives with the CLI are discussed next.

A. Static - manual configuration

We first must set or create a number of IPv4 address objects. It is assumed here that the interface used for Internet connection is **G2**, the ISP gateway IPv4 address is *10.5.4.1*, the IPv4 address for the connecting interface will be *10.5.4.35* and the network to which they both belong is *10.5.4.0/24*.

Note: Private IPv4 addresses are used for example only

Each installation's IP addresses will be different from the example IP addresses but they are used here only to illustrate how setup is done. Also, these addresses are private IPv4 addresses and in reality an ISP would use public IPv4 addresses instead.

We first add the gateway IPv4 address object which we will call *wan_gw*:

```
Device:/> add Address IP4Address wan_gw Address=10.5.4.1
```

This is the address of the ISP's gateway which is the first router hop towards the public Internet. If this IP object already exists, it can be given the IP address with the command:

```
Device:/> set Address IP4Address wan_gw Address=10.5.4.1
```

Now use this object to set the gateway on the **G2** interface which is connected to the ISP:

```
Device:/> set Interface Ethernet G2 DefaultGateway=wan_gw
```

Next, set the IP object *G2_ip* which will be the IPv4 address of the interface connected to the ISP:

```
Device:/> set IP4Address InterfaceAddresses/G2_ip Address=10.5.4.35
```

Note: Qualifying the names of IP objects in folders

*On initial startup of the E7, cOS Core automatically creates and fills the **InterfaceAddresses** folder in the cOS Core address book with Ethernet interface related IPv4 address objects.*

*When an IP address object which is located in a folder is specified in the CLI, the object name must be qualified with the name of its parent folder. For example, to reference the address **G2_ip**, it must be qualified with the folder name **InterfaceAddresses** so it becomes **InterfaceAddresses/G2_ip**.*

If an object is not contained in a folder and is at the top level of the address book then no qualifying parent folder name is needed.

Now, set the IP object *G2_net* which will be the IP network of the connecting interface:

```
Device:/> set IP4Address InterfaceAddresses/G2_net Address=10.5.4.0/24
```

It is recommended to verify the properties of the **G2** interface with the command:

```
Device:/> show Interface Ethernet G2
```

The typical output from this will be similar to the following:

```
                  Property  Value
 -------------------------  -------------------------
                      Name:  G2
                        IP:  InterfaceAddresses/G2_ip
                   Network:  InterfaceAddresses/G2_net
            DefaultGateway:  wan_gw
                 Broadcast:  10.5.4.255
                 PrivateIP:  <empty>
                     NOCHB:  <empty>
                       MTU:  1500
                    Metric:  100
               DHCPEnabled:  No
```

```
           EthernetDevice:  0:G2  1:<empty>
         AutoSwitchRoute:  No
AutoInterfaceNetworkRoute:  Yes
  AutoDefaultGatewayRoute:  Yes
  ReceiveMulticastTraffic:  Auto
     MemberOfRoutingTable:  All
                 Comments:  <empty>
```

Setting the default gateway on the interface has the additional effect that cOS Core automatically creates a route in the default *main* routing table that has the network *all-nets* routed on the interface. This means that we do not need to explicitly create this route.

Even though an *all-nets* route is automatically added, no traffic can flow without the addition of an *IP rule* which explicitly allows traffic to flow. Let us assume we want to allow web browsing from the protected network *G3_net* on the interface **G3**. A simple rule to do this would have the rule's *Action* property set to the value *Allow* and is defined with the following command:

The IP rule set *main* always exists by default and is a top level CLI context. Add an IP rule called *lan_to_wan* to allow the traffic through to the public Internet:

```
Device:/> add IPRule name=lan_to_wan
                        Action=Allow
                        SourceInterface=G3
                        SourceNetwork=InterfaceAddresses/G3_net
                        DestinationInterface=G2
                        DestinationNetwork=all-nets
                        Service=http-all
```

This IP rule would be correct if the internal network hosts have public IPv4 addresses but in most scenarios this will not be true and internal hosts will have private IPv4 addresses. In that case, we must use NAT to send out traffic so that the apparent source IP address is the IP of the interface connected to the ISP. To do this we simply change the *Action* property in the above command from a value of *Allow* to a value of *NAT*:

```
Device:/main> add IPRule name=lan_to_wan
                        Action=NAT
                        SourceInterface=G3
                        SourceNetwork=InterfaceAddresses/G3_net
                        DestinationInterface=G2
                        DestinationNetwork=all-nets
                        Service=http-all
```

The service used in the IP rule is *http-all* which will allow most web browsing but does not include the DNS protocol to resolve URLs into IP addresses. To solve this problem, a custom service could be used in the above rule which combines *http-all* with the *dns-all* service. However, the recommended method which provides the most clarity to a configuration is to create a separate IP rule for DNS:

```
Device:/main> add IPRule name=lan_to_wan_dns
                        Action=NAT
                        SourceInterface=G3
                        SourceNetwork=InterfaceAddresses/G3_net
                        DestinationInterface=G2
                        DestinationNetwork=all-nets
                        Service=dns-all
```

It is recommended that at least one DNS server is also defined in cOS Core. This DSN server or servers (a maximum of three can be configured) will be used when cOS Core itself needs to resolve URLs which will be the case when a URL is specified in a configuration instead of an IP address. If we assume an IP address object called *dns1_address* has already been defined for the first DNS server, the command to specify the first DNS server is:

```
Device:/> set DNS DNSServer1=dns1_address
```

Assuming a second IP object called *dns2_address* has been defined, the second DNS server is specified with:

```
Device:/> set DNS DNSServer2=dns2_address
```

B. DHCP - automatic configuration

Alternatively, all required IP addresses can be automatically retrieved from the ISP's DHCP server by enabling DHCP on the interface connected to the ISP. If the interface on which DHCP is to be enabled is **G2**, then the command is:

```
Device:/> set Interface Ethernet G2 DHCPEnabled=Yes
```

Once the required IP addresses are retrieved with DHCP, cOS Core automatically sets the relevant address objects in the address book with this information.

For cOS Core to know on which interface to find the public Internet, a *route* has to be added to the *main* cOS Core routing table which specifies that the network *all-nets* can be found on the interface connected to the ISP and this route must also have the correct *Default Gateway* IP address specified. This *all-nets* route is added automatically by cOS Core during the DHCP address retrieval process. Automatic route generation is a setting for each interface that can be manually enabled and disabled.

After all IP addresses are set via DHCP and an *all-nets* route is added, the connection to the Internet is configured but no traffic can flow to or from the Internet since there is no IP rule defined that allows it. As was done in the previous option (**A**) above, we must therefore manually define an IP rule that will allow traffic from a designated source interface and source network (in this example, the network *G3_net* and interface **G3**) to flow to the destination network *all-nets* and the destination interface **G2**.

C. PPPoE setup

For PPPoE connection, create the PPPoE tunnel interface on the interface connected to the ISP. The interface **G2** is assumed to be connected to the ISP in the command shown below which creates a PPPoE tunnel object called *wan_ppoe*:

```
Device:/> add Interface PPPoETunnel wan_ppoe
                        EthernetInterface=G2
                        username=pppoe_username
                        Password=pppoe_password
                        Network=all-nets
```

The ISP will supply the correct values for *pppoe_username* and *pppoe_password* in the dialog above.

The PPPoE tunnel interface can now be treated exactly like a physical interface by the policies defined in cOS Core rule sets.

There also has to be a route associated with the PPPoE tunnel to allow traffic to flow through it and this is automatically created in the *main* routing table when the tunnel is defined. If the PPPoE tunnel object is deleted, this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated

source interface and source network (in this example, the network *G3_net* and interface **G3**) to flow to the destination network *all-nets* and the destination interface which is the PPPoE tunnel that has been defined.

D. PPTP setup

For PPTP connection, first create the PPTP tunnel interface. It is assumed below that we will create a PPTP tunnel object called *wan_pptp* with the remote endpoint *10.5.4.1*:

```
Device:/> add Interface L2TPClient wan_pptp
                        Network=all-nets
                        username=pptp_username
                        Password=pptp_password
                        RemoteEndpoint=10.5.4.1
                        TunnelProtocol=PPTP
```

Your ISP will supply the correct values for *pptp_username*, *pptp_password* and the remote endpoint.

Your ISP will supply the correct values for *pptp_username*, *pptp_password* and the remote endpoint. An interface is not specified when defining the tunnel because this is determined by cOS Core looking up the *Remote Endpoint* IP address in its routing tables.

The PPTP client tunnel interface can now be treated exactly like a physical interface by the policies defined in cOS Core rule sets.

There also has to be an associated route with the PPTP tunnel to allow traffic to flow through it, and this is automatically created in the *main* routing table when the tunnel is defined. The destination network for this route is the *Remote Network* specified for the tunnel and for the public Internet this should be *all-nets*.

As with all automatically added routes, if the PPTP tunnel object is deleted then this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source interface and source network (in this example, the network *G3_net* and interface **G3**) to flow to the destination network *all-nets* and the destination interface which is the PPTP tunnel that has been defined.

Activating and Committing Changes

After any changes are made to a cOS Core configuration, they will be saved as a new configuration but will not yet be activated. To activate all the configuration changes made since the last activation of a new configuration, the following command must be issued:

```
Device:/> activate
```

Although the new configuration is now activated, it does not become permanently activated until the following command is issued within 30 seconds following the *activate*:

```
Device:/> commit
```

The reason for two commands is to prevent a configuration accidentally locking out the administrator. If a lock-out occurs then the second command will not be received and cOS Core will revert back to the original configuration after the 30 second time period (this time period is a setting that can be changed).

DHCP Server Setup

If the Clavister Security Gateway is to act as a DHCP server then this can be set up in the following way:

First define an IPv4 address object which has the address range that can be handed out. Here, we will use the IPv4 range *192.168.1.10 - 192.168.1.20* as an example and this will be available on the **G3** interface which is connected to the protected internal network *G3_net*.

```
Device:/> add Address IP4Address dhcp_range
                      Address=192.168.1.10-192.168.1.20
```

The DHCP server is then configured with this IP address object on the appropriate interface. In this case we will call the created DHCP server object *dhcp_lan* and assume the DHCP server will be available on the **G3** interface:

```
Device:/> add DHCPServer dhcp_lan
                      IPAddressPool=dhcp_range
                      Interface=G3
                      Netmask=255.255.255.0
                      DefaultGateway=InterfaceAddresses/G3_ip
                      DNS1=dns1_address
```

It is important to specify the *Default gateway* for the DHCP server since this will be handed out to DHCP clients on the internal network so that they know where to find the public Internet. The default gateway is always the IP address of the interface on which the DHCP server is configured. In this case, *G3_ip*.

NTP Server Setup

Network Time Protocol (NTP) servers can optionally be configured to maintain the accuracy of the system date and time. The command below sets up synchronization with the two NTP servers at hostname *pool.ntp.org* and IPv4 address *10.5.4.76*:

```
Device:/> set DateTime TimeSyncEnable=Yes
               TimeSyncServer1=dns:pool.ntp.org
               TimeSyncServer2=10.5.4.76
```

The prefix *dns:* is added to the hostname to identify that it must resolved to an IP address by a DNS server (this is a convention used in the CLI with some commands).

Syslog Server Setup

Although logging may be enabled, no log messages are captured unless a server is set up to receive them and *Syslog* is the most common server type. If the Syslog server's address is *195.11.22.55* then the command to create a log receiver object called *my_syslog* which enables logging is:

```
Device:/> add LogReceiverSyslog my_syslog IPAddress=195.11.22.55
```

Allowing ICMP *Ping* Requests

As a further example of setting up IP rules, it can be useful to allow ICMP *Ping* requests to flow through the Clavister Security Gateway. As discussed earlier, cOS Core will drop any traffic unless an IP rule explicitly allows it. Let us suppose that we wish to allow the pinging of external hosts with the ICMP protocol by computers on the internal *G3_net* network. The commands to allow this are as follows.

Add an IP rule called *allow_ping_outbound* to allow ICMP pings to pass:

```
Device:/> add IPRule name=allow_ping_outbound
                        Action=NAT
                        SourceInterface=G3
                        SourceNetwork=InterfaceAddresses/G3_net
                        DestinationInterface=G2
                        DestinationNetwork=all-nets
                        Service=ping-outbound
```

The IP rule again has the *NAT* action and this is necessary if the protected local hosts have private IPv4 addresses. The ICMP requests will be sent out from the Clavister Security Gateway with the IP address of the interface connected to the ISP as the source interface. Responding hosts will send back ICMP responses to this single IP and cOS Core will then forward the response to the correct private IP address.

Adding a Drop All Rule

Scanning of the IP rule set is done in a top-down fashion. If **no** matching IP rule is found for a new connection then the *default rule* is triggered. This rule is hidden and cannot be changed and its action is to drop all such traffic as well as generate a log message for the drop.

In order to gain control over the logging of dropped traffic, it is recommended to create a drop all rule as the last rule in the *main* IP rule set. This rule has an *Action* of *Drop* with the source and destination network set to *all-nets* and the source and destination interface set to *any*.

The service for this rule must also be specified and this should be set to *all_services* in order to capture all types of traffic. The command for creating this rule is:

```
Device:/main> add IPRule name=drop_all
                        Action=Drop
                        SourceInterface=any
                        SourceNetwork=any
                        DestinationInterface=any
                        DestinationNetwork=all-nets
                        Service=all_services
```

A valid license should now be installed to remove the cOS Core 2 hour demo mode limitation. Doing this is described in *Section 4.5, "License Installation Methods"*.

4.5. License Installation Methods

Without a valid license installed, cOS Core will run in *demo mode* (demonstration mode) which means that it will cease to function after two hours of operation. Restarting cOS Core will re-enable cOS Core for another two hours. To remove this 2 hour restriction, a valid license must be installed.

Licenses are files which are made available for download from the Clavister servers but before they become available, the user must have registered themselves with Clavister and doing this is described in *Chapter 2, Registering with Clavister*.

Installation Methods

The following methods can be used for installing the first cOS Core license in the E7 unit:

- **Automatically through the Setup Wizard**

  As described in *Section 4.2, "Web Interface and Wizard Setup"*, when the wizard is used for initially configuring Clavister hardware, the administrator can choose to install a license as one of the wizard steps.

  This method is also only available when installing a license for the first time.

- **Automatically through the Web Interface**

  Go to **Status > Maintenance > License** and enter the customer's login credentials for the Clavister website, then press **Activate**. The license is fetched automatically across the public Internet and installed.

  This method is also only available when installing a license for the first time.

- **Automatically through the CLI**

  In the CLI, enter the command:

  ```
  Device:/> license -activate -request -username=myname -password=mypass
  ```

  The customer username and password login are included in the command and the license is fetched automatically across the Internet. The login credentials are the same ones that are used for Clavister website login. The *reconf* or *shutdown* command should be used to complete installation.

  This method is also only available when installing a license for the first time.

- **Manually through the Web Interface or SCP**

  This method is the only choice when the E7 hardware does not have a connection to the public Internet. The procedure consists of the following steps:

  i. In a web browser, go to the Clavister website at ***https://www.clavister.com***, select **Log in** and then log in to the site. This will require registration on the site if this has not been done already.

  ii. Go to **Licenses > Register License**.

  iii. Select the option **Register by Service Tag and Hardware Serial Number**.

  iv. Enter the *Serial Number* and *Service Tag* codes. For Clavister hardware products, these codes are found on a label on the unit.

v. Download a license from the license list to the computer's local disk.

vi. The license file is uploaded to the security gateway through the cOS Core Web Interface by going to **Status > Maintenance > License** and pressing the **Upload** button to select the license file. Following upload, cOS Core will install the file.

Alternatively, the license file can be uploaded using SCP. cOS Core automatically recognizes an uploaded license file but it is then necessary to manually to perform a reconfigure or reboot operation to complete installation.

Important: Restart is recommended after license installation

After installing a license, a restart of cOS Core is recommended. This will ensure that cOS Core memory is correctly configured for the license parameters.

*When installing a license through the Web Interface or the startup wizard, the option to restart will be presented. When using the CLI or SCP for installation, restarting is done. in the Web Interface by going to **Status > Maintenance > Reset & Restore**. With the CLI, use the command:*

```
Device:/> shutdown -reboot
```

Installing Future Licenses

As mentioned above, fetching the license automatically using the setup wizard, Web Interface or CLI is only possible for the first time a license is installed. After that, future license installations can only be performed using the following two methods:

- Manually, by logging into and downloading from the Clavister website and then uploading manually to cOS Core.
- Automatically through the separate InControl software product which is used for managing cOS Core configurations. This method can also be used to install the first license.

Licenses and license installation are described further in the separate *cOS Core Administrators Guide*.

4.6. Setup Troubleshooting

This appendix deals with connection problems that might occur when connecting a management workstation to a Clavister Security Gateway.

If the management interface does not respond after the Clavister Security Gateway has powered up and cOS Core has started, there are a number of simple steps to troubleshoot basic connection problems:

1. Check that the correct interface is being used.

The most obvious problem is that the wrong Clavister Security Gateway interface has been used for the initial connection. Only the first interface found by cOS Core is activated for the initial connection from a browser after cOS Core starts for the first time.

2. Check that interface characteristics match.

If a Clavister Security Gateway's interface characteristics are configured manually then the interface on a switch to which it is connected should be configured with the same characteristics. For instance, the link speeds and half/full duplex settings must match. If they do not, communication will fail. This problem will not occur if the interfaces are set for automatic configuration on both sides and automatic is always the Clavister factory default setting.

3. Check that the workstation IP is configured correctly.

The second most obvious problem is if the IP address of the workstation running the web browser is not configured correctly.

4. Is the management interface properly connected?

Check the link indicator lights on the management interface. If they are dark then there may be a cable problem.

5. Using the *ifstat* CLI command.

To investigate a connection problem further, connect the a console to the local console port on the Clavister Security Gateway. Once cOS Core has started, it should respond with the a standard CLI prompt when the enter key is pressed. Now enter the following command once for each interface:

```
Device:/> ifstat <if-name>
```

Where *<if-name>* is the name of the management interface. This will display a number of counters for that interface. The *ifstat* command on its own can list the names of all the interfaces.

If the *Input* counters in the hardware section of the output are not increasing then the error is likely to be in the cabling. However, it may simply be that the packets are not getting to the Clavister Security Gateway in the first place. This can be confirmed with a packet sniffer if it is available.

If the *Input* counters are increasing, the management interface may not be attached to the correct physical network. There may also be a problem with the routing information in any connected hosts or routers.

6. Using the *arpsnoop* CLI command.

A final diagnostic test is to try using the console command:

```
Device:/> arpsnoop all
```

This will display console messages that show all the *ARP* packets being received on the different interfaces and confirm that the correct cables are connected to the correct interfaces. To look at the ARP activity only a particular interface, follow the command with the interface name:

```
Device:/> arpsnoop <interface>
```

To switch snooping off, use the command:

```
Device:/> arpsnoop none
```

4.7. Going Further with cOS Core

After initial setup is complete, the administrator is ready to go further with configuring cOS Core to suit the requirements of a particular networking scenario. All E7 resources can be downloaded from the E7 product page which can be found at ***http://www.clavister.com/start***.

The primary reference documentation consists of:

- The cOS Core Administrators Guide
- The cOS Core CLI Reference Guide
- The cOS Core Log Reference Guide
- The cOS Core Application Control Signatures

The cOS Core Administrators Guide

This guide is a comprehensive description of all cOS Core features and includes a detailed table of contents with a comprehensive index to quickly locate particular topics.

Examples of the setup for various scenarios are included but screenshots are kept to a minimum since the user has a variety of management interfaces to choose from.

Basic cOS Core Objects and Rules

As a minimum, the new administrator should become familiar with the cOS Core *Address Book* for defining IP address objects and with the cOS Core *IP rule set* for defining *IP Rule* objects which allow or block different traffic and which can also be used to set up NAT address translation.

IP rules identify the targeted traffic using combinations of the source/destination interface/network combined with protocol type. By default, no IP rules are defined so all traffic is dropped. At least one IP rule needs to be defined before traffic can traverse the Clavister Security Gateway.

An alternative to *IP Rule* objects is to use *IP Policy* objects. These have essentially the same function but simplify the setting up of address translation and the use of important functions such as application control, virus scanning and web content filtering.

In addition to rules, *Route* objects need to be defined in a *Routing Table* so that traffic can be sent on the correct interface to reach its final destination. Traffic will need both a relevant rule and route to exist in order for it to traverse the security gateway.

ALGs

Once the address book and IP rules are understood, the various ALGs will probably be relevant for managing higher level protocols such as HTTP. For example, for management of web browsing, the HTTP ALG provides a number of important features such as content filtering. Using *IP Policy* objects can remove the need to use ALGs as separate objects.

VPN Setup

A common requirement is to quickly setup VPN networks based on Clavister Security Gateways. The *cOS Core Administrators Guide* includes an extensive VPN section and as part of this, a *VPN Quick Start* section which goes through a checklist of setup steps for nearly all types of VPN scenarios.

Included with the quick start section is a checklist for troubleshooting and advice on how best to deal with the networking complications that can arise with certificates.

Log Messages

By default, certain events will generate log messages and at least one log server should be configured in cOS Core to capture these messages, although a feature called *memlog* will capture recent log messages in local cOS Core memory. The administrator should review what events are important to them and at what severity. The *cOS Core Log Reference Guide* provides a complete listing of the log messages that cOS Core is capable of generating.

The CLI Reference Guide

The *CLI Reference Guide* provides a complete listing of the available CLI commands with their options. A CLI overview is also provided as part of the *cOS Core Administrators Guide*.

cOS Core Education Courses

For details about classroom and online cOS Core education as well as cOS Core certification, visit the Clavister company website at *http://www.clavister.com* or contact your local sales representative.

Staying Informed

Clavister maintains an RSS feed of announcements that can be subscribed to at *https://forums.clavister.com/rss-feeds/announcements/*. It is recommended to subscribe to this feed so that you receive notifications when new releases of cOS Core versions are available for download and installation. Alternatively, announcements can be read directly from the Clavister forums which can be found at *https://forums.clavister.com/*.

Chapter 5: Resetting to Factory Defaults

In some circumstances, it may be necessary to reset the E7 hardware to the state it was in when it left the factory. This is known as a *reset to factory defaults*.

With the E7, a factory reset is only possible via the software *boot menu*. There is no manual reset button on the hardware itself. The boot menu can only be accessed through the local CLI console after the E7 is powered up and can be entered by pressing any console key before cOS Core has fully started.

Note: Any console password will be reset to no password

If a console password was set this will also be reset to the factory default of no password. If required, the console password should be set later by choosing the boot menu option ***Enable Console Password****.*

Performing a Boot Menu Reset

The E7 does not provide a hardware reset button on the hardware unit itself. Instead, the reset is done by entering the hardware's *boot menu*. A boot menu reset is done with the following steps:

1. Make sure a separate management computer running as a console is attached to the local console port of the E7.
2. Power up the E7 unit. This may require a restart if the hardware is already powered up.
3. As the first console output appears, press any console key before cOS Core has fully started.
4. The *boot menu* will now be displayed on the console.
5. Choose the menu item **Reset Options**.
6. Various reset options are now displayed on the console. For a full reset, select the menu option **Reset to Factory Defaults**.

A complete description of the boot menu and its options can be found in the separate *cOS Core Administrators Guide*.

Warning: Current configuration and cOS Core upgrades are lost

The factory defaults will include the default configuration and the original version of cOS Core that the product left the factory with.

This means:

- *The current cOS Core configuration will be lost but can be restored if a backup is available.*
- *Any cOS Core upgrades that have been performed since the product left the factory will be lost. An upgrade to a newer cOS Core version must be repeated.*

Chapter 6: Warranty Service

Limitation of Warranty

Clavister warrants to the customer of the E7 Appliance that the Hardware components will be free from defects in material and workmanship under normal use for a period of two (2) years from the Start Date (as defined below). The warranty will only apply to failure of the product if Clavister is informed of the failure not later than two (2) years from the Start Date or thirty (30) days after that the failure was or ought to have been noticed by the customer.

The warranty will not apply to products from which serial numbers have been removed or to defects resulting from unauthorized modification, operation or storage outside the environmental specifications for the product, in-transit damage, improper maintenance, defects resulting from use of third-party software, accessories, media, supplies, consumables or such items not designed for use with the product, or any other misuse. Any replacement Hardware will be warranted for the remainder of the original warranty period or thirty days, whichever is longer.

Note that the term "*Start Date*" means the earlier of the product registration date **OR** ninety (90) days following the day of shipment by Clavister.

Obtaining Warranty Service with an RMA

Warranty service can be obtained within the warranty period with the following steps:

1. Obtain a ***Return Material Authorization*** **(RMA) Number** from Clavister. This number **must** be obtained before the product is sent back.

   The Clavister RMA request form can be found online at (clickable link):

   http://www.clavister.com/support/support-center/

   If the Purchaser's circumstances require special handling of warranty correction, then at the time of requesting the RMA number, the Purchaser may also propose suitable special procedures.

2. The defective product **MUST** be packaged securely in the original packaging or other suitable shipping packaging to ensure that it will not be damaged in transit.

3. The RMA number must be clearly marked on the outside of the package.

4. The package is then shipped to Clavister with all the costs of mailing/shipping/insurance paid by the Purchaser. The address for shipping is:

Clavister AB
Sjögatan 6J
891 60 Örnsköldsvik
SWEDEN

If the product has not yet been registered with the Clavister through its client web, a proof of purchase (such as a copy of the dated purchase invoice) must be provided with the shipped product.

Important: An RMA Number must be obtained before shipping!

Any package returned to Clavister without an RMA number will be rejected and shipped back to the Purchaser at the Purchaser's expense. Clavister reserves the right in such a case to levy a reasonable handling charge in addition to mailing and/or shipping costs.

Data on the Hardware

Note that Clavister is not responsible for any of the purchaser's software, firmware, information, or memory data contained in, stored on, or integrated with any product returned to Clavister pursuant to this warranty.

Contacting Clavister

Should there be a problem with the online form then Clavister support can be contacted by email at: *support@clavister.com*.

Hardware Replacement Procedures

Details of procedures for replacing old Clavister hardware can be found in the separate Clavister document: *Hardware Replacement Guide for cOS Core 10.nn*. A new license must be obtained for the new unit using the standard procedure.

Customer Remedies

Clavister's entire liability according to this warranty shall be, at Clavister's option, either return of the price paid, or repair or replacement of the Hardware that does not meet Clavister's limited warranty and which is returned to Clavister with a copy of your receipt.

Limitations of Liability

Refer to the legal statement at the beginning of the guide for a statement of liability limitations.

Chapter 7: Safety Precautions

Safety Precautions

Clavister E7 devices are *Safety Class I* products and have protective ground terminals. There must be an uninterrupted safety earth ground from the main power source to the product's input wiring terminals, power cord, or supplied power cord set. Whenever it is likely that the protection has been impaired, disconnect the power cord until the ground has been restored.

For LAN cable grounding:

- If your LAN covers an area served by more than one power distribution system, be sure their safety grounds are securely interconnected.
- LAN cables may occasionally be subject to hazardous transient voltage (such as lightning or disturbances in the electrical utilities power grid). Handle exposed metal components of the network with caution.

There are no user-serviceable parts inside these products. Only service-trained personnel can perform any adjustment, maintenance or repair.

Säkerhetsföreskrifter

Dessa produkter är säkerhetsklassade enligt klass I och har anslutningar för skyddsjord. En obruten skyddsjord måste finnas från strömkällan till produktens nätkabelsanslutning eller nätkabel. Om det finns skäl att tro att skyddsjorden har blivit skadad, måste produkten stängas av och nätkabeln avlägnas till dess att skyddsjorden har återställts.

För LAN-kablage gäller dessutom att:

- om LAN:et täcker ett område som betjänas av mer än ett strömförsörjningssystem måste deras respektive skyddsjord vara ihopkopplade.
- LAN kablage kan vara föremål för farliga spänningstransienter (såsom blixtnedslag eller störningar i elnätet). Hantera metallkomponenter i förbindelse med nätverket med försiktighet.

Det finns inga delar i produkten som kan lagas av användaren. All service samt alla justeringar, underhåll eller reparationer får endast utföras av behörig personal.

Informations concernant la sécurité

Cet appareil est un produit de classe I et possède une borne de mise à la terre. La source d'alimentation principale doit être munie d'une prise de terre de sécurité installée aux bornes du câblage d'entree, sur le cordon d'alimentation ou le cordon de raccordement fourni avec le produit. Lorsque cette protection semble avoir été endommagée, débrancher le cordon d'alimentation jusqu'à ce que la mise à la terre ait été réparée.

Mise à la terre du câble de réseau local:

- si votre réseau local s'étend sur une zone desservie par plus d'un système de distribution de puissance, assurez-vous que les prises de terre de sécurité soint convenablement interconnectées.
- Les câbles de réseaux locaux peuvent occasionnellement être soumis à des surtensions transitoires dangereuses (telles que la foudre ou des perturbations dans le réseau d'alimentation public). Manipulez les composants métalliques du réseau avec précautions.

Aucune pièce contenue à l'intérieur de ce produit ne peut être réparée par l'utilisateur. Tout dépannage, réglage, entretien ou réparation devra être confié exclusivement à un personnel qualifié.

Hinweise zur Sicherheit

Dies ist ein Gerät der Sicherheitsklasse I und verfügt über einen schützenden Erdungsterminal. Der Betrieb des Geräts erfordert eine ununterbrochene Sicherheitserdung von der Hauptstromquelle zu den Geräteingabeterminals, den Netzkabeln oder dem mit Strom belieferten Netzkabelsatz voraus. Sobald Grund zur Annahme besteht, dass der Schutz beeinträchtigt worden ist, das Netzkabel aus der Wandsteckdose herausziehen, bis die Erdung wiederhergestellt ist.

Für LAN-Kabelerdung:

- Wenn Ihr LAN ein Gebiet umfasst, das von mehr als einem Stromverteilungssystem beliefert wird, müssen Sie sich vergewissern, dass die Sicherheitserdungen fest untereinander verbunden sind.
- LAN-Kabel können gelegentlich gefährlichen Übergangsspannungen ausgesetz werden (beispielsweise durch Blitz oder Störungen in dem Starkstromnetz des Elektrizitätswerks). Bei der Handhabung exponierter Metallbestandteile des Netzwerkes Vorsicht walten lassen.

Dieses Gerät enthält innen keine durch den Benutzer zu wartenden Teile. Wartungs-, Anpassungs-, Instandhaltungs- oder Reparaturarbeiten dürfen nur von geschultem Bedieningspersonal durchgeführt werden.

Considerazioni sulla sicurezza

Questo prodotte è omologato nella classe di sicurezza I ed ha un terminale protettivo di collegamento a terra. Dev'essere installato un collegamento a terra di sicurezza, non interrompibile che vada dalla fonte d'alimentazione principale ai terminali d'entrata, al cavo d'alimentazione oppure al set cavo d'alimentazione fornito con il prodotto. Ogniqualvolta vi sia probabilità di danneggiamento della protezione, disinserite il cavo d'alimentazione fino a quando il collegaento a terra non sia stato ripristinato.

Per la messa a terra dei cavi LAN:

- se la vostra LAN copre un'area servita da più di un sistema di distribuzione elettrica, accertatevi che i collegamenti a terra di sicurezza siano ben collegati fra loro;
- i cavi LAN possono occasionalmente andare soggetti a pericolose tensioni transitorie (ad esempio, provocate da lampi o disturbi nella griglia d'alimentazione della società elettrica); siate cauti nel toccare parti esposte in metallo della rete.

Nessun componente di questo prodotto può essere riparato dall'utente. Qualsiasi lavoro di riparazione, messa a punto, manutenzione o assistenza va effettuato esclusivamente da personale specializzato.

Consideraciones sobre seguridad

Este aparato se enmarca dentro de la clase I de seguridad y se encuentra protegido por una borna de puesta a tierra. Es preciso que exista una puesta a tierra continua desde la toma de alimentacíon eléctrica hasta las bornas de los cables de entrada del aparato, el cable de alimentación hasta haberse subsanado el problema.

Puesta a tierra del cable de la red local (LAN):

- Si la LAN abarca un área cuyo suministro eléctrico proviene de más de una red de distribución de electricidad, cerciorarse de que las puestas a tierra estén conectadas entre sí de modo seguro.
- Es posible que los cables de la LAN se vean sometidos de vez en cuando a voltajes momentáneos que entrañen peligro (rayos o alteraciones en la red de energía eléctrica). Manejar con precaución los componentes de metal de la LAN que estén al descubierto.

Este aparato no contiene pieza alguna susceptible de reparación por parte del usuario. Todas las reparaciones, ajustes o servicio de mantenimiento debe realizarlos solamente el técnico.

Appendix A: E7 Specifications

Below are the key hardware specifications for the Clavister E7 product.

Dimensions, Weight and MTBF

Height x Width x Depth (mm)	40 x 280 x 200
Hardware Weight	1.74 kg
Hardware Form Factor	Desktop
19-inch Rack Mountable	Yes, using rack mounting kit
MTBF	Base unit: 807,862 hours @ 40° C External power supply: 60,000 hours @ 40° C

Regulatory and Safety Standards

Safety	UL, CE
EMC	FCC class A, CE class A, UL

Environmental

Operating and Storage Humidity	5% to 95% noncondensing
Operating Temperature	0 to 35° C
Vibration	0.41 Grms2 (3-500 Hz)
Mechanical Shock	30 G

Power Specifications

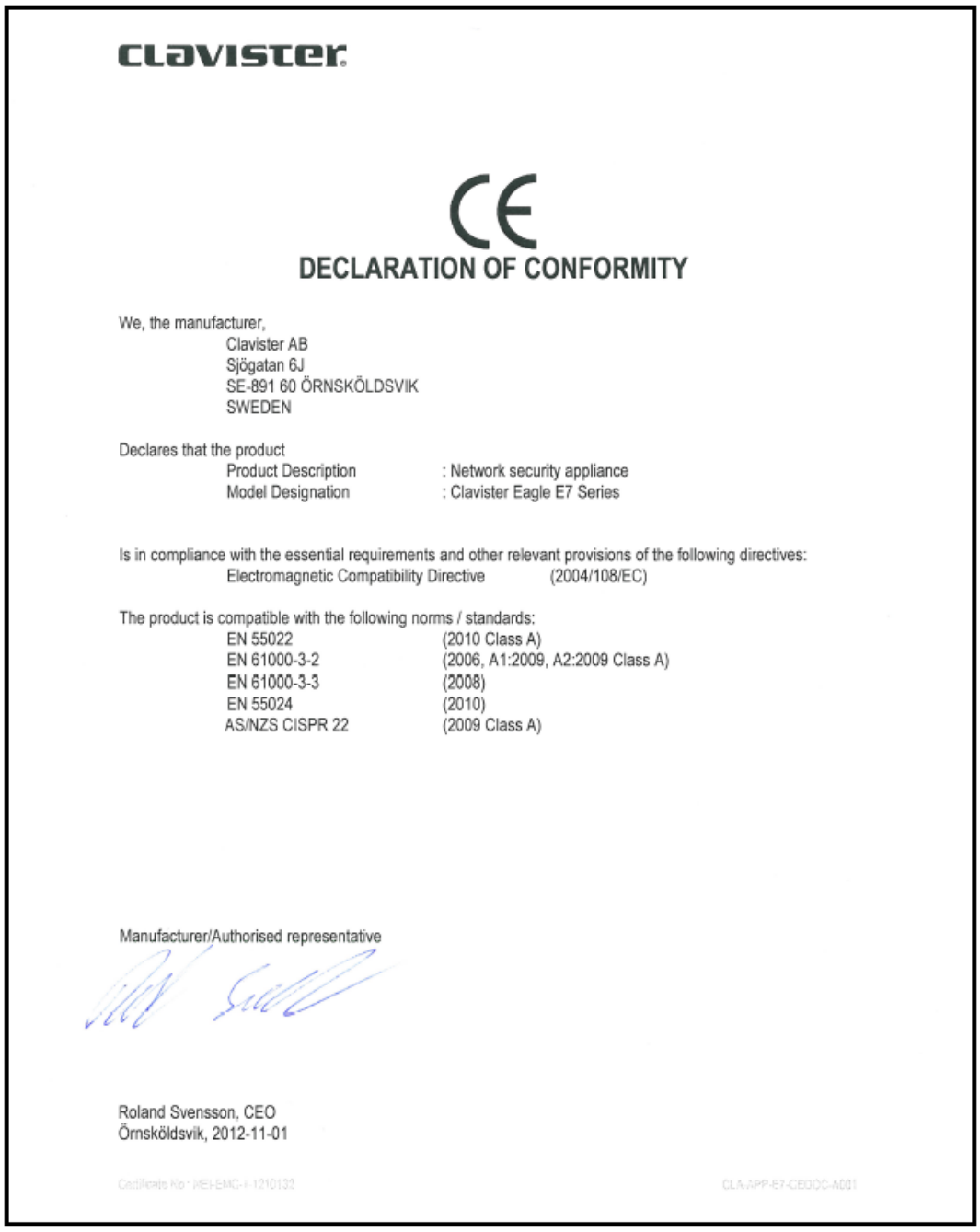
Power Supply (AC)	90-264 VAC, 50-60 Hz
Typical Power Consumption	14 W
Typical Current @ 230V	90 mA
BTU	48 BTU
PSU Rated Power	36 to 40 W
Appliance Input	12 VDC

Ethernet Interface Support

Gigabit RJ45 interfaces	Automatic MDI-X 1000BASE-T (copper RJ45 100m) 100BASE-TX (copper RJ45 100m) 10BASE-T (copper RJ45 100m)

For more information about Clavister products, go to: *http://www.clavister.com*.

Appendix B: Declarations of Conformity



clavister

CE

DECLARATION OF CONFORMITY

We, the manufacturer,

Clavister AB
Sjögatan 6J
SE-891 60 ÖRNSKÖLDSVIK
SWEDEN

Declares that the product

Product Description	: Network security appliance
Model Designation	: Clavister Eagle E7 Series

Is in compliance with the essential requirements and other relevant provisions of the following directives:

Electromagnetic Compatibility Directive (2004/108/EC)

The product is compatible with the following norms / standards:

EN 55022	(2010 Class A)
EN 61000-3-2	(2006, A1:2009, A2:2009 Class A)
EN 61000-3-3	(2008)
EN 55024	(2010)
AS/NZS CISPR 22	(2009 Class A)

Manufacturer/Authorised representative

Roland Svensson, CEO
Örnsköldsvik, 2012-11-01

Certificate No: MEI-EMC-I-1210133 CLA-APP-E7-CEDOC-A001

clavister

DECLARATION OF CONFORMITY

We, the manufacturer,

Clavister AB
Sjögatan 6J
SE-891 60 ÖRNSKÖLDSVIK
SWEDEN

Declares that the product

Product Description	: Desktop Network Security Appliance
Model Designation	: Clavister Eagle E7 Series

Is in compliance with the essential requirements and other relevant provisions of the following:

FCC CFR Title 47 Part 15 Subpart B: 2010	Federal Communication Commission Code of Federal Regulations Telecommunications, Radio frequency devices, unintentional radiators
Canadian Standards Association Standard ICES-003 Issue 5: 2012	Spectrum Management and Telecommunications Policy Interference- Causing Equipment Standard, Digital Apparatus

The product is compatible with the following norms / standards:

FCC CFR Title 47 Part 15 Subpart B Class A: 2010
CSA ICES-003 Issue 5: 2012
CISPR 22: 2008
CAN/CSA-CISPR 22-10

Manufacturer/Authorised representative

Roland Svensson, CEO
Örnsköldsvik, 2012-11-01

Certificate No.: NEI-FCCE-1-1210132 CLA-APP-E7-FCCDOC A001

NOTICE OF COMPLETION AND AUTHORIZATION TO APPLY THE UL MARK

11/02/2012

Cameo Communications Inc
Ms. Anita Chang
276 Sinhu 1st Rd
Neihu District
Taipei 114, Tw

Our Reference:	File E159561, Vol. X2	Project Number	12CA55650
Your Reference:	C0561210031		
Project Scope:	UL/CUL Investigation, Desktop Network Security Appliance, Model CLAVISTER EAGLE E7 SERIES		

Dear Ms. Anita Chang:

Congratulations! UL's investigation of your product(s) has been completed under the above Reference Number and the product was determined to comply with the applicable requirements. This letter temporarily supplements the UL Follow-Up Services Procedure and serves as authorization to apply the UL Mark at authorized factories under UL's Follow-Up Service Program. To provide your manufacturer(s) with the intended authorization to use the UL Mark, you must send a copy of this notice to each manufacturing location currently authorized under File E159561, Vol. X2.

Records in the Follow-Up Services Procedure covering the product are now being prepared and will be sent in the near future. Until then, this letter authorizes application of the UL Mark for 90 days from the date indicated above.

Additional requirements related to your responsibilities as the Applicant can be found in the document "Applicant responsibilities related to Early Authorizations" that can be found at the following web-site:
http://www.ul.com/EAResponsibilities

Any information and documentation provided to you involving UL Mark services are provided on behalf of UL LLC (UL) or any authorized licensee of UL.

We are excited you are now able to apply the UL Mark to your products and appreciate your business. Feel free to contact me or any of our Customer Service representatives if you have any questions.

Very truly yours,

Bruno Chen
+886 2 28967790
Engineer Project Associate
Bruno.Chen@ul.com

Reviewed by:

William R. Carney
847/664-1088
Chief Engineer Director I
William.R.Carney@ul.com

CC: PERFECTLINK INTERNATIONAL CORP, MS. JEAN CHANG

TPIA682-783F29

This is an electronically generated letter. Signatures are not required for this document to be valid.

Page 1 of 1

Appendix C: Port Based VLAN Setup

VLAN support on the E7 is divided into two types:

- On the Ethernet interfaces **G1**, **G2** and **G3**, VLANs are created by configuring them normally in cOS Core. It is cOS Core that then takes on the task of adding and recognizing VLAN tags in packets. It is not a hardware function.

  Setting up these types of VLAN with the E7 is discussed in the separate *cOS Core Administration Guide*.

- For the E7 **GESW** interfaces only (numbered **1** to **8**), VLANs are configured in cOS Core in a different way.

  All the **GESW** interfaces are connected together by a common hardware switch fabric and this fabric also takes care of managing the packet tagging for any VLANs configured on the interfaces. This allows the ability to configure *Port Based VLANs*.

  This appendix describes configuring port based VLANs for of the **GESW** interfaces.

The arrangement of VLANs on the **GESW** interfaces has the following characteristics:

- Each of the E7 **GESW** interfaces has the possibility of being a separate VLAN or part of a VLAN group.
- The E7 **GESW** interfaces can be grouped together onto VLANs with arbitrary numbers of physical ports in each VLAN. For example, the interfaces could be divided so that the first 2 interfaces are part of one VLAN, the next 2 interfaces are part of a second VLAN and the remainder are left in normal operation.
- The **GESW** interfaces that are not part of a VLAN will continue to operate as a single interface with the logical interface name **GESW**.

Configuring VLANs

How to configure port based VLANs will be illustrated with an example. Assume that the requirement is to divide the **GESW** interfaces as follows:

- The first interface will continue to operate normally through the switch fabric. This will therefore be the logical cOS Core interface **GESW**.
- The **GESW** interfaces **2**, **3** and **4** will become three separate VLANs with the logical names **gesw_port2**, **gesw_port3** and **gesw_port4**.
- The remaining four **GESW** interfaces **5**, **6**, **7** and **8** will become a single VLAN with the logical name **gesw_port5-8**.

To configure these VLANs, perform the following steps in the Web Interface:

1. Define the VLAN objects

In the Web Interface, go to **Network > Interfaces and VPN > VLAN > Add** and add four new *VLAN* objects. Each VLAN should have an arbitrary value assigned for the *VLAN ID*, *IP Address* and *Network* properties. Only the *VLAN ID* needs to be unique for the **GESW** interface. The IP addresses should not be public IPv4 addresses.

A screenshot of how the resulting VLAN list might look in the Web Interface is shown below.

#	Name	Interface	VLAN ID	IPv4 Address	IPv6 Address	Network
1	gesw_port2	gesw	200	192.168.20.1		192.168.20.0/24
2	gesw_port3	gesw	300	192.168.30.1		192.168.30.0/24
3	gesw_port4	gesw	400	192.168.40.1		192.168.40.0/24
4	gesw_port5-8	gesw	500	192.168.50.1		192.168.50.0/24

2. Associate the VLANs with GESW interfaces

Go to **Network > Interfaces and VPN > VLAN > Switch Management**, enable port based VLAN and set each numbered **GESW** interface to be associated with the relevant VLAN to get the desired configuration.

For this example, the screenshot below shows how this would look in the Web Interface.

This last dialog is only available in the Web Interface for Clavister hardware platforms that support port based VLANs.

Port Based VLAN Issues

There are some issues which the adminstrator should be aware of when setting up port based VLANs:

- **Port based VLANs cannot be mixed with VLAN trunks.**

  When the port based VLAN feature is used, **all** of the **GESW** interfaces act as access ports and none can be used for 802.1q VLAN trunks.

- **MAC addresses are duplicated.**

  The MAC addresses of all the **GESW** interfaces are the same. This means that a switch might have two connections to the security gateway that have two different IP addresses but the same MAC address. For some switches this can be a problem and the situation should be avoided by using separate switches.

clavister®

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
www.clavister.com